ISSN 2447-1097

Direito & TI – Porto Alegre / RS www.direitoeti.com.br

A PANDEMIA DO CIBERCRIME

Nágila Magalhães Cardoso[1]

RESUMO

O esperado ano de 2020, que parecia no imaginativo de muitas pessoas um roteiro futurista de grandes inovações tecnológicas, tornou-se uma realidade totalmente inesperada, preocupante e insegura. Em meio a uma das maiores ameaças da humanidade, o novo Corona-Vírus deixou às claras a vulnerabilidade decorrente enfrentada. Proporcionou aos cibercriminosos apenas mais uma oportunidade para práticas delituosas, aliada a uma população fragilizada e que estão mais tempo on-line em suas casas, buscando por informações relacionadas a pandemia, além de usarem a tecnologia para se comunicar com a família, na realização de trabalhos, compras, pagamentos e entretenimento. A nova rotina despertou o apetite dos golpistas lucrarem em tempos de crise. Esse é o campo de análise do presente artigo.

Palavras-chave: cibercrime; coronavirus; golpe; pandemia.

INTRODUÇÃO

A criminalidade cibernética já existe há um bom tempo, até então não é nenhuma novidade, o avanço, a decorrência da facilidade da utilização da internet e dos recursos tecnológicos tornaram infelizmente um campo atrativo e bastante comum para exploração de crimes. O novo cenário do isolamento social, medida essa recomendada pela Organização Mundial da Saúde em circunstância da pandemia do COVID-19, inevitavelmente transformou a rotina de milhões de pessoas, que estas passaram a ter que se adaptar às pressas com a nova realidade e realizar suas tarefas de suas casas por meio do ambiente virtual que passou então a ser questão de sobrevivência, entretanto local este cheio de armadilhas principalmente para os menos inexperientes.

É duro imaginar na situação a qual estamos vivenciando, o caos na saúde, que existe indivíduos empenhados, se aproveitando do momento de fragilidade para cometer delitos na rede, na verdade precisamos ser bem realistas em dizer que nem no mundo dos sonhos, os usuários da internet podem navegar tranquilamente pela web, sem ser atraídos por armadilhas de golpistas digitais.

Um relatório recentemente feito pela Unit 42[i], a área de pesquisa da empresa Palo Alto Networks, foram detectados, milhares (de fato mais de 100.000) domínios registrados contendo termos como "covid", "vírus" e "corona". Identificamos 116.357 domínios recém-registrados com nomes relacionados à corona vírus entre 1º de janeiro e 31 de março. Desses, 2.022 são classificados como “maliciosos” e mais de 40.000 são considerados de “alto risco”. Além disso, de 1º de fevereiro a 31 de março, testemunhamos um crescimento de 569% nos registros de domínios maliciosos. [1]

[1] Tecnóloga, professora de informática, colunista. Esp. Segurança Computacional. E-mail: nagilamagalhaes@gmail.com. Currículo Lattes: http://lattes.cnpq.br/3024752858194202.

Os aumentos significativos só nos comprovam como sempre, o que não é nenhuma novidade, golpistas que veem os tempos de crise, como pandemias e desastres naturais, juntamente com qualquer outro ambiente de medo a oportunidade para cometer fraudes eletrônicas.

1 A OPORTUNIDADE FAZ O LADRÃO

Pesquisas como pandemia, corona vírus, covid 19, vacina, remédio para corona vírus, álcool, mascaras, filmes ou séries sobre epidemias, auxilio emergencial, internet gratuita, estas tem sido algumas das indicações que a nossa curiosidade, ansiedade e medo estão registrando excessivamente nas ferramentas de buscas na internet, o próprio público e o seu fator humano tem contribuído expressivamente para os cibercriminosos o melhor caminho a ser seguido para os seus ataques que através de links fraudulentos baseados nessas buscas, vem atraindo e iludindo cada vez mais vítimas em meio a quarentena.

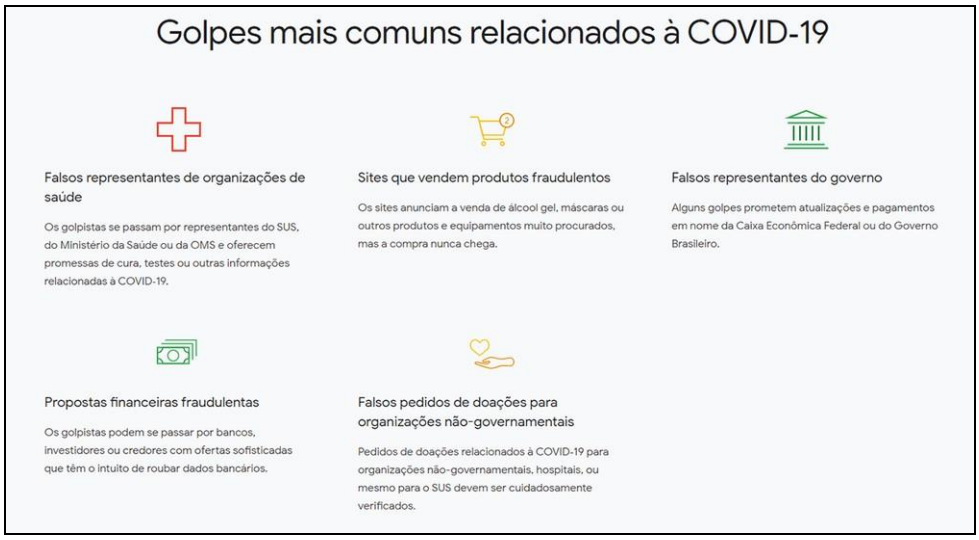
"O diretor de operações da Apura, Maurício Paranhos, diz que os crimes cibernéticos, que já vinham em ascensão, se multiplicaram após o início da pandemia. "Os cibercriminosos estão utilizando temas relacionados à Covid para chamar a atenção e atacar. Não poupam nem instituições de saúde".[ii]

Para a Unit 42, os criminosos estão provendo ataques com as seguintes táticas:

> **Webshops falsos:** sites fraudulentos que ofereciam itens de alta demanda, como máscaras faciais ou desinfetantes para as mãos, por um preço com desconto.
> **Armadilha de cartão de crédito:** scripts em outras lojas maliciosas que vendem produtos relevantes para pandemia para roubar informações de cartão de crédito.
> **E-books falsos:** domínios criados para explorar o medo do consumidor e forçá-los a comprar ebooks sobre COVID-19 reproduzindo um vídeo sobre as situações e eventos mais assustadores relacionados à pandemia.
> **Farmácias ilícitas:** sites não licenciados e que utilizam sites comprometidos que usam nomes de domínio, sugerindo a venda de remédios para o COVID-19, quando na verdade anunciam Viagra e outros medicamentos não relacionados ao vírus. [2]

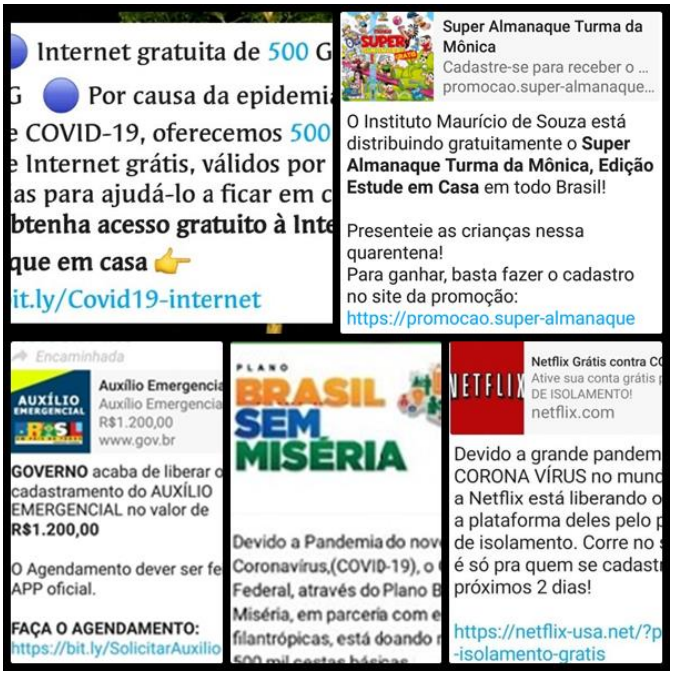
Na mesma linha de pesquisa o Google divulga os cinco golpes mais comuns na web envolvendo a pandemia da Covid-19 (Figura 1).[iii]

Figura 1. Golpes mais comuns relacionados à COVID-19. **Fonte:** Google



Observa-se a seguir alguns exemplos reais de golpes mais proliferados na rede.

Figura 2. Golpes da pandemia **Fonte:** Google Imagens



2 O RISCO DO HOMEOFFICE

A necessidade do isolamento social fez com que as empresas e as instituições optassem às pressas pelo serviço remoto, o termo em alta utilizado, “Home-Office” a modalidade do trabalho

remoto, passou a ser um dos principais pilares de sustentação do mercado e prioridade em prol da saúde dos funcionários retirando estes das instalações físicas da empresa para as instalações físicas da sua própria casa, dando assim continuidade no desenvolvimento dos serviços com "segurança," mas convenhamos que as medidas de isolamento nos protege do vírus biológico lá fora, mas não das ameaças do vírus humano cibercriminoso.

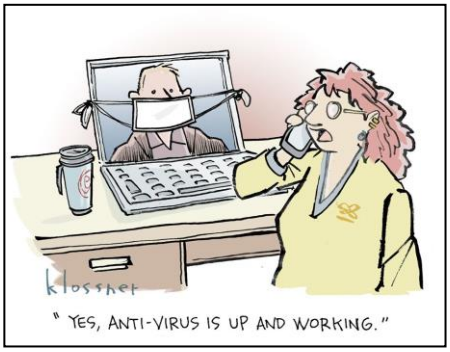
Algumas pessoas poderiam até já estarem acostumadas ao trabalho remoto, entretanto uma boa parte declaram- se "nômades digitais" ou inexperientes com a nova forma de trabalho, que podem estar nesse exato momento em qualquer local do planeta realizando suas atividades e mesmo sem intenção, colocando a empresa em risco, o agravante passa então a serem esses colaboradores, o elo mais fraco em questão, considerando uma presa fácil para os caçadores virtuais do crime.

Os larápios digitais já perceberam que o dinheiro "de verdade" está nos ataques a redes corporativas que muitas das vezes são acessadas pelos usuários a partir de dispositivos desprotegidos, que podem ser muito mais eficazes e destruidores do que aqueles voltados aos usuários comuns.

> A entrega rápida de aparelhos aos funcionários, ou então, a liberação de redes internas para acesso remoto, com trabalhadores usando as próprias máquinas para o expediente. "Esses dispositivos não estão mais sob o controle dos departamentos de TI, e por isso, podem acabar sendo vetores para ataques", explica o especialista.
> Assolini aponta ainda o fato de que muita gente não tem o conhecimento necessário para cuidar da própria segurança ou simplesmente não se importa com isso. O resultado é o acesso a partir de redes desprotegidas ou roteadores mal configurados, a falta de atualização de sistemas operacionais ou a ausência de softwares de segurança, como antivírus ou malwares. Em todos os casos, são portas abertas para a entrada de malwares ou a aplicação de golpes.[Ii]

Com a pandemia, os bandidos também passaram a trabalhar ainda mais de home office. Para se ter ideia de acordo com a IBM e-mails maliciosos subiram 600% em março, após alta do home office. A figura 3 a seguir, ilustra uma sátira da realidade atual.[iv]

Figura 3. Antivírus está funcionando. **Fonte:** Global Digital Forensics



Diante dessa situação surgi o questionamento, será que as empresas estão devidamente preparadas para o trabalho remoto em grande escala? Políticas, processos e normas que definem e orientam diretrizes de segurança foram criados ou revisados? e equipamentos, ferramentas e dispositivos tecnológicos foram adaptados para suportar esta nova realidade? O que colaboradores podem ou não devem fazer ao utilizar seus próprios dispositivos pessoais para trabalhar? É necessário utilizar ferramentas, ou medidas de segurança específicas? Estas são apenas algumas reflexões sobre os atuais desafios.

CONSIDERAÇÕES FINAIS

Podemos constatar nesse caos pandêmico ou em qualquer outra situação de calamidade pública o quão benéfico para humanidade é a utilização das tecnologias como reposta a alternativas e possibilidades de um enfrentamento a uma crise ou não. Gera- se então a reflexão de quantas vezes a tecnologia foi capaz de salvar vidas? A gente está salvando essas vidas ficando em casa, quando deixamos a tecnologia ser nossa maior aliada, optando, por exemplo: fazer transações bancarias pelo internet banking ao invés de se deslocar até uma agencia bancaria, fazer compras via internet, ou uma simples mensagem no WhatsApp e aguardar o delivery, usar uma plataforma virtual para reuniões, amenizar a saudade de pessoas queridas através de uma chamada de vídeo, a telemedicina, teleaula, teletrabalho entre outras infinidades de coisas, tudo isso realizado graças o intermédio da tecnologia, evitando assim o índice maior de contagio viral dessas inúmeras idas e vindas fora de nossas casas. Já parou para pensar, se conseguirmos ficar mais tempo em casa, é pela tecnologia.

Acredito que para muitos, inúmeros são os desafios e descobertas que fazem parte da nova realidade com a adoção mais intensificada da tecnologia, mas o imprescindível no mundo da tecnologia, é procurar manter-se sempre que possível atualizado, ou seja, ter o nosso antigo e precioso habito que já temos fora do ambiente virtual, que é estar atualizado com as notícias, ter atenção, o cuidado ao sair nas ruas, ao falar com estranhos. As medidas de quem navega no ciberespaço, são as mesmas recomendadas de quem anda nas ruas. Inevitavelmente na mesma proporção que caminha os avanços no mundo digital, caminha também em alta os avanços do crime, criminosos que não dorme no ponto estão se evoluindo constantemente e atualizando com as tendências, aprimorando suas ferramentas cada vez mais poderosas para atacar, invadir, acessar indevidamente e obter dados e informações que sejam rentáveis.

Portanto a atenção não deve ser somente para profissionais de segurança e tecnologia, mas principalmente para cidadãos de um mundo em constante transformação. Entretanto não basta somente isso, é necessário mais políticas públicas voltadas para a questão, mais abrangência nos meios de

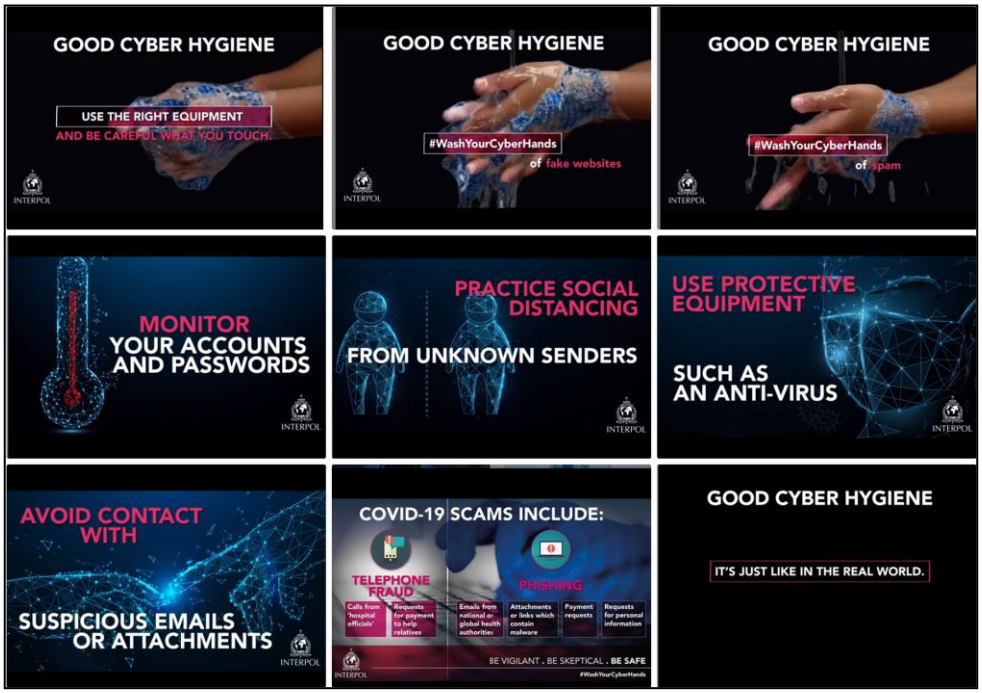
comunicação, órgãos e empresas mais empenhada em educar, conscientizar de alguma forma as pessoas. A criminalidade digital ainda não é suficientemente tratada com um certo grau de relevância, o que deixa na mente de algumas pessoas a falsa visão de que as coisas que acontecem no virtual fica somente por lá ou pela incredulidade humana de que aquela tal conduta criminosa não será capaz de acontecer e me causar danos.

Nota-se um certo esforço dos órgãos governamentais e demais instituições, ações no combate do novo corona vírus, através das mídias de comunicação em relação aos cuidados que devem ser adotados ao uso de mascaras, as medidas do distanciamento social, higienização correta das mãos, entre outras dicas de prevenção, com o propósito de conscientizar a população, evitando o aumento de infecções e consequentemente o número de mortes pela Covid-19.

De maneira semelhante deveria haver informações à população com dicas de segurança para que não houvesse o crescimento de vítimas lesadas por golpes digitais, que não ficasse restrito apenas em canais de comunicação sobre tecnologia ou da polícia por exemplo.

A campanha inspiradora da Interpol por meio de imagens e vídeos (Figura 4), difundida nas redes sociais com a 'hashtag' #WashYourCyberHands (Lave Suas Mãos Cibernéticas), tem como objetivo divulgar boas práticas de "higiene virtual", para evitar ataques, devido ao confinamento de decretado em muitos países [v]. Iniciativas como estas que sempre foram tratadas também como prioritárias em outros países. Quando o Brasil irá levar a sério isso? Quando é que o Brasil irá fazer uma campanha como esta, para ser exibida em comercial televisivo?

Figura 4. Campanha Lave Suas Mãos Cibernéticas. **Fonte:** Instagram Interpol Hq



REFERÊNCIAS

Alfasi, S. **COVID-19, Info Stealer & the Map of Threats – Threat Analysis Report**. Disponívem em: https://blog.reasonsecurity.com/2020/03/09/covid-19-info-stealer-the-map-of-threats-threat-analysis-report/. Acesso em: 18 jun. 2020.

Dermatini, F. Coronavírus - **Golpe promete Netflix de graça, mas quer roubar seus dados**. Disponível em: https://canaltech.com.br/seguranca/netflix-gratis-golpe-coronavirus-162332/. Acesso em: 18 jun. 2020

Demartini, F. **Isolamento e home office levaram a aumento em ataques de ransomware no Brasil.** Disponível em: https://canaltech.com.br/hacker/isolamento-e-home-office-levaram-a-aumento-em-ataques-de-ransomware-no-brasil-162463/. Acesso em: 18 jun. 2020.

Lusa. **Campanha da Interpol alerta para o crime cibernético durante a pandemia**. Disponível em: https://www.noticiasaominuto.com/mundo/1473135/campanha-da-interpol-alerta-para-o-crime-cibernetico-durante-a-pandemia. Acesso em: 18 jun. 2020.

Olson, R. **Don't Panic: COVID-19 Cyber Threats.** Disponível em: https://unit42.paloaltonetworks.com/covid19-cyber-threats/. Acesso em: 18 jun. 2020.

Rohr, A. **Google lista tipos de golpes na web mais comuns durante a pandemia- Veja dicas para não cair neles**. Disponível em: https://g1.globo.com/economia/tecnologia/blog/altieres-rohr/post/2020/05/01/google-lista-tipos-de-golpes-na-web-mais-comuns-durante-a-pandemia-veja-dicas-para-nao-cair-neles.ghtml. Acesso em: 18 jun. 2020

Sutto, G. **Golpe do auxílio emergencial atinge mais de 11 milhões de pessoas- Caixa dá dicas de como evitar.** Disponível em: https://www.infomoney.com.br/minhas-financas/golpe-do-auxilio-emergencial-atinge-mais-de-11-milhoes-de-pessoas-caixa-da-dicas-de-como-evitar/. Acesso em: 18 jun. 2020.

Tauhata, S., Moreira, T. **E-mails maliciosos subiram 600% em março, após alta do home office, diz IBM.** Disponível em: https://valorinveste.globo.com/produtos/servicos-financeiros/noticia/2020/06/10/e-mails-maliciosos-aumentaram-600percent-em-marco-apos-aumento-do-home-office-diz-executivo-da-ibm.ghtml. Acesso em: 18 jun. 2020.

Vieira, E. **Trabalho Remoto: Riscos e Estratégias- Reflexões de um mundo em constantes transformações.** Disponível em: https://media.datacenterdynamics.com/media/documents/TRABALHO_REMOTO_-_RISCOS_E_ESTRATEGIAS_DCD_ABR_2020_versao_PDF.pdf. Acesso em: 18 jun. 2020.

---

[i] OLSON, Ryan. Don't Panic: COVID-19 Cyber Threats. Disponível em: https://unit42.paloaltonetworks.com/covid19-cyber-threats/. Acesso em: 18 jun. 2020.

[ii] DEMARTINI, Felipe. Isolamento e home office levaram a aumento em ataques de ransomware no Brasil. Disponível em:< https://canaltech.com.br/hacker/isolamento-e-home-office-levaram-a-aumento-em-ataques-de-ransomware-no-brasil-162463/>. Acesso em: 18 jun. 2020.

[iii] ROHR, Altieres. Google lista tipos de golpes na web mais comuns durante a pandemia; veja dicas para não cair neles. Disponivel em:< https://g1.globo.com/economia/tecnologia/blog/altieres-rohr/post/2020/05/01/google-lista-tipos-de-golpes-na-web-mais-comuns-durante-a-pandemia-veja-dicas-para-nao-cair-neles.ghtml>. Acesso em: 18 jun. 2020.

[iv] TAUHATA, Sergio. MOREIRA, Talita. E-mails maliciosos subiram 600% em março, após alta do home office, diz IBM. Disponível em:< https://valorinveste.globo.com/produtos/servicos-financeiros/noticia/2020/06/10/e-mails-maliciosos-aumentaram-600percent-em-marco-apos-aumento-do-home-office-diz-executivo-da-ibm.ghtml>. Acesso em: 18 jun. 2020.

[v] LUSA. Campanha da Interpol alerta para o crime cibernético durante a pandemia. Disponível em: <https://www.noticiasaominuto.com/mundo/1473135/campanha-da-interpol-alerta-para-o-crime-cibernetico-durante-a-pandemia>. Acesso em: 18 jun. 2020.

[1] In the past few weeks, thousands (in fact over 100,000) of domains have been registered containing terms like “covid,” “virus”, and “corona.”
We’ve identified 116,357 newly registered domains with coronavirus-related names between January 1 and March 31. Out of these, 2,022 are classified as “malicious” and more than 40,000 are considered “high-risk”. Additionally, from February 1 to March 31, we witnessed a 569% growth in malicious domain registrations.

[2] Fake webshops: Scam websites that offered high-demand items like face masks or hand sanitizers for a discounted price.
Credit card skimmers: Scripts on other malicious stores that sell pandemic-relevant goods to steal credit card information.
Fake ebooks: Domains set up to prey into consumer fear and coerce them into buying COVID-19 ebooks by playing a video about the scariest situations and events related to the pandemic.
Illicit pharmacies: Unlicensed and leverage compromised websites that use domain names suggesting they sell remedies for COVID-19 when they actually advertise Viagra and other drugs unrelated to the virus.