ILMA. SRA. DRA. DELEGADA DE POLÍCIA TITULAR
DO 78º DISTRITO POLICIAL DE SÃO PAULO - SP

AUTOS Nº 1506068-38.2020.8.26.0050

CLEO PIRES AYROSA GALVÃO, vítima já qualificada nos autos do Inquérito Policial em epígrafe, vem, respeitosamente, por seus advogados, à presença de Vossa Senhoria, requerer a juntada do **Estudo** (Doc. 01) em anexo, que analisou os riscos presentes no link (site) postado pelo invasor no Instagram (@Cleo) de propriedade da vítima, e que foi clicado por mais de 600 mil seguidores, tudo conforme abaixo:

1. O presente estudo (Doc. 01), acostado, realizado por um especialista em segurança da informação, faz uma análise dos riscos que teriam sido expostos os seguidores da Cleo e, também, qual seria o principal objetivo do invasor.

2. Segundo este estudo, o *modus operandi* do criminoso é invadir o perfil das celebridades e, aproveitando-se dos milhões de seguidores (como no caso da Cleo), oferecer um falso prêmio (neste caso Iphones), para que tais seguidores acessem um link, postado por este criminoso, no perfil invadido.

3. Quando o seguidor/usuário clica neste link, ele é direcionado a uma página, que lhe solicita a realização de alguma tarefa, download ou verificação, para chegar ao prêmio anunciado.

4. Na verdade o prêmio inexiste, e o seguidor/usuário nunca chegará à página que lhe confere tal prêmio, uma vez que sempre será solicitada a realização de uma nova tarefa.

5. Pela realização destas tarefas, downloads, verificações ou cliques, por estes seguidores/usuários, é que o criminoso obtém remuneração.

6. Explico: alguns serviços e sites pagam por cliques ou tarefas realizadas em determinados links (serviço este absolutamente legal), todavia, o criminoso utiliza-se destes serviços, objetivando ganhar dinheiro ilicitamente. Invade conta nas redes sociais, cria falsa entrega de prêmios e aproveita-se dos cliques ou tarefas realizadas pelos seguidores das celebridades invadidas, que acessaram o link postado por ele.

7. Vale dizer, de acordo com este estudo, **o objetivo do criminoso é fazer com que os seguidores da celebridade invadida (como os da Cleo) cliquem no link postado por ele e realizem tarefas virtuais, com isto o criminoso ganha dinheiro e consuma seu golpe**.

8. Com base no estudo juntado, o **criminoso/invasor não tem intenção de atacar ou invadir os dispositivos dos seguidores da Cleo**, pois nenhum risco de instalação de vírus, coleta de senhas ou dados pessoais foi encontrado.

9. Isto posto, o estudo concluiu que: ***"os mais de 600 mil seguidores, que acessaram o link postado pelo criminoso no Instagram @Cleo, não tiveram seus dispositivos expostos à riscos, invasões ou coleta de dados"*** e ***"se fizeram algum download de aplicativo apontado no site, estes vieram de meios de distribuição oficiais e foram previamente revisados e aprovados pelas plataformas oficiais".***

10. Derradeiramente, caso os seguidores tenham clicado em algum outro link, constante da página divulgada pelo invasor, o estudo também apontou que estes seguidores "**apenas receberam propostas publicitárias".**

11. Considerando a propriedade do Estudo apresentado, é que se requer sua juntada, como subsídio à investigação em curso, neste Inquérito Policial presidido por Vossa Senhoria, para fim de Direito.

Termos em que,
pede deferimento.

São Paulo, 28 de maio de 2020.

(assinado digitalmente)
LUIZ AUGUSTO FILIZZOLA D'URSO
OAB/SP nº 369.000

(assinado digitalmente)
LUIZ FLÁVIO BORGES D'URSO
OAB/SP nº 69.991

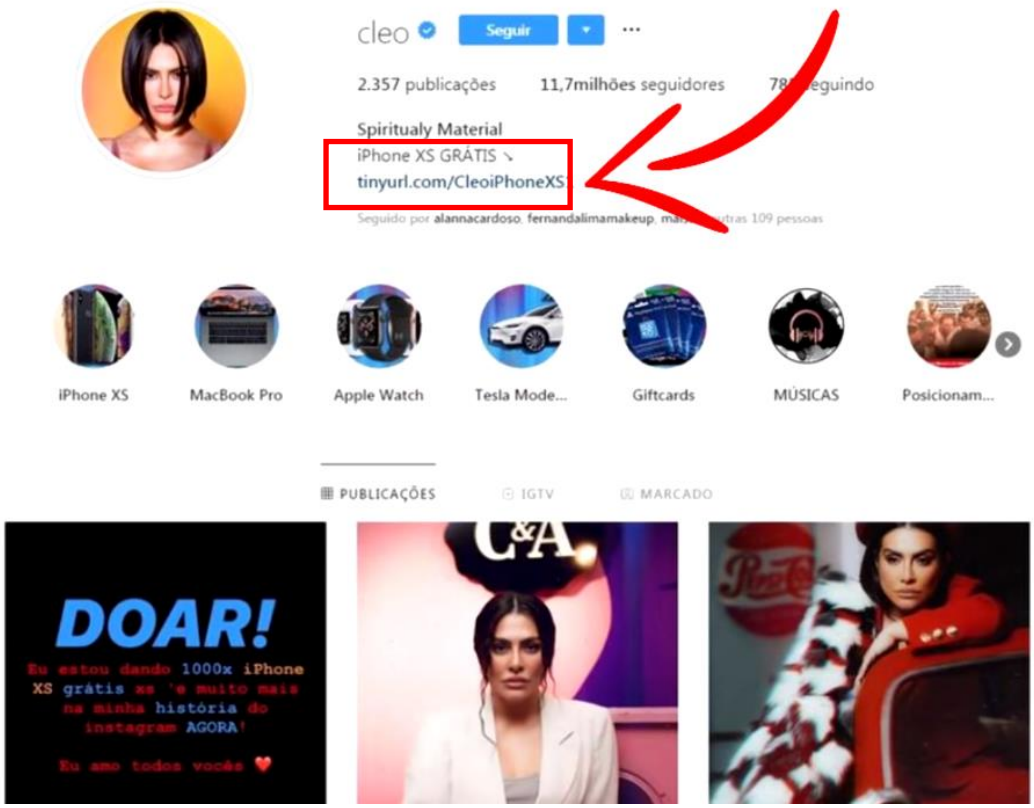
(DOC. 01)

ESTUDO SOBRE O LINK POSTADO POR INVASOR NO INSTAGRAM @CLEO

**Gabriel Pato*
São Paulo, 27 de maio de 2020

1. A atriz Cleo teve seu Instagram invadido em 16/10/19, sendo que o invasor postou nos "*Stories*" e também no "*Feed*", da conta da atriz, uma suposta doação de 1.000 Iphones XS.

2. Para receber esta doação de Iphone, o seguidor precisava clicar em um determinado link e seguir alguns passos, como apresentados a seguir:



3. Este link direcionava os usuários a uma página pertencente a uma rede de distribuição de anúncios, que irei analisar neste estudo.

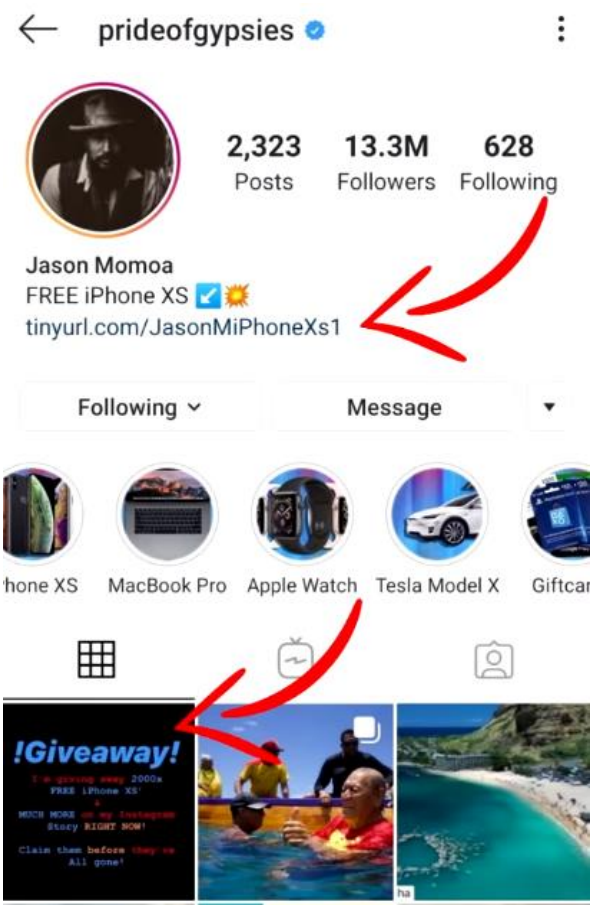
4. Além disso, em pesquisa, verifiquei que este tipo de invasão e postagem ocorreu com outros famosos (todos com milhões de seguidores no Instagram), tanto brasileiros como estrangeiros. Todos posts com mesmo estilo de letra, cor, texto e etc. Vejamos:

Ludmilla (Cantora):

Marina Ruy Barbosa (Atriz):

Robert Downey Jr. (Ator americano mundialmente conhecido):

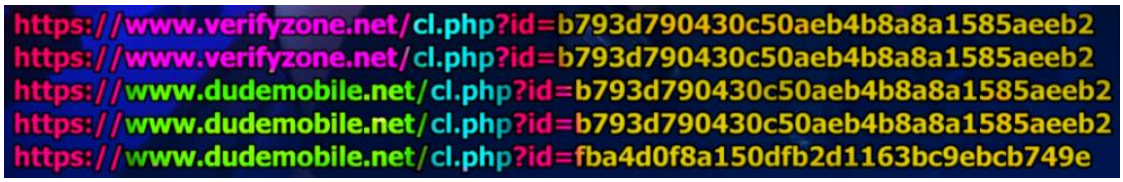
Jason Momoa (Ator americano):



5. Resume-se aqui todos os links postados por este invasor ou invasores, nos perfis destes famosos:

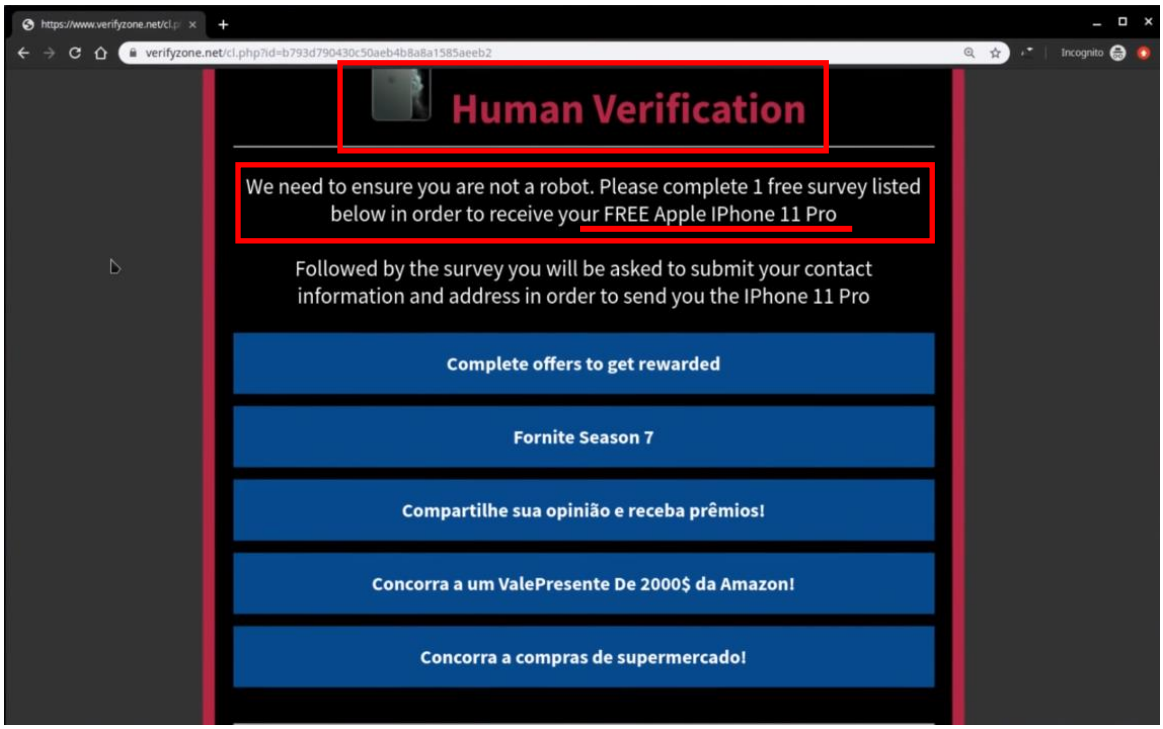
6. Todos estes endereços web utilizam-se de encurtadores, vale dizer, links encurtados e alterados por um serviço disponível de maneira gratuita e livre para todos os usuários na Internet, não sendo, portanto, o destino final do link.

7. Após análise mais aprofundada, revelam-se os destinos finais de tais links, quais sejam:



8. Todos estes links resultam em serviços e nos mesmos “ids” ou em um similar, e em páginas norte-americanas, o que indica que referidas invasões possivelmente foram realizadas pelo mesmo criminoso ou mesmo grupo, e que, pela utilização de serviços estrangeiros e pela precária escrita da língua portuguesa, aparentemente, tais criminosos são estrangeiros.

9. A referida rede de distribuição de anúncios (que era acessada por aqueles que clicavam nos links postados pelos criminosos, no Instagram dos famosos) trabalha com um modelo de negócios no qual se solicita aos visitantes realizar uma determinada tarefa antes de poderem acessar o conteúdo final, **vale dizer, para ganhar o suposto Iphone, o usuário precisa realizar uma atividade anterior e provar que não é um “robô”**, vejamos:



10. Este modelo é conhecido como "*content locker*". Apesar da empresa e do modelo de negócios serem legítimos, entendo que o invasor a tenha utilizado, de maneira ilícita, para monetizar sua invasão.

11. O criminoso, utilizando este serviço, consegue ganhar dinheiro com a realização destas tarefas/downloads/atividades/verificações por aqueles (seguidores) que clicam no link que ele mesmo (invasor) postou no Instagram da vítima invadida, como ocorrido no caso da Cleo.

12. Acredita-se que os usuários irão realizar tais atividades, pois querem ganhar o Iphone, e estes entendem que só os ganharão após realizar estas atividades/verificações, e assim, com tais tarefas realizadas, o criminoso consegue ganhar dinheiro.

13. É incalculável a quantidade de usuários que realizaram tais tarefas e a quantia recebida pelo criminoso. No caso da Cleo, o link teve mais de 600 mil cliques pelos seus seguidores, todavia, não é possível mensurar quantos usuários realizaram tais tarefas/atividades requisitadas no site.

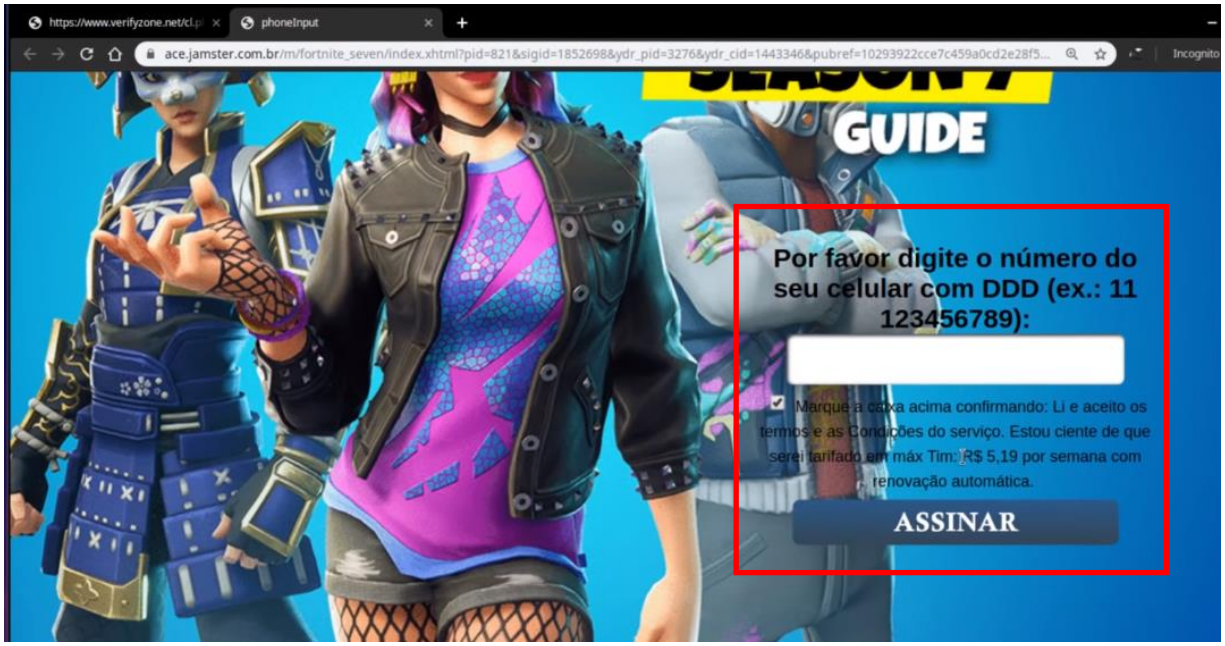
14. Dentre as tarefas/atividades solicitadas, a principal era o download de aplicativos de celular, sendo que, o invasor era remunerado cada vez que um usuário fazia a instalação e executava um destes aplicativos listados no site.

15. Estes aplicativos eram legítimos e os downloads eram feitos nas lojas oficiais de aplicativos dos principais sistemas operacionais mobile (como a Play Store para Android, e App Store para iOS), **sendo assim, todos os aplicativos foram revisados e analisados conforme as regras das**

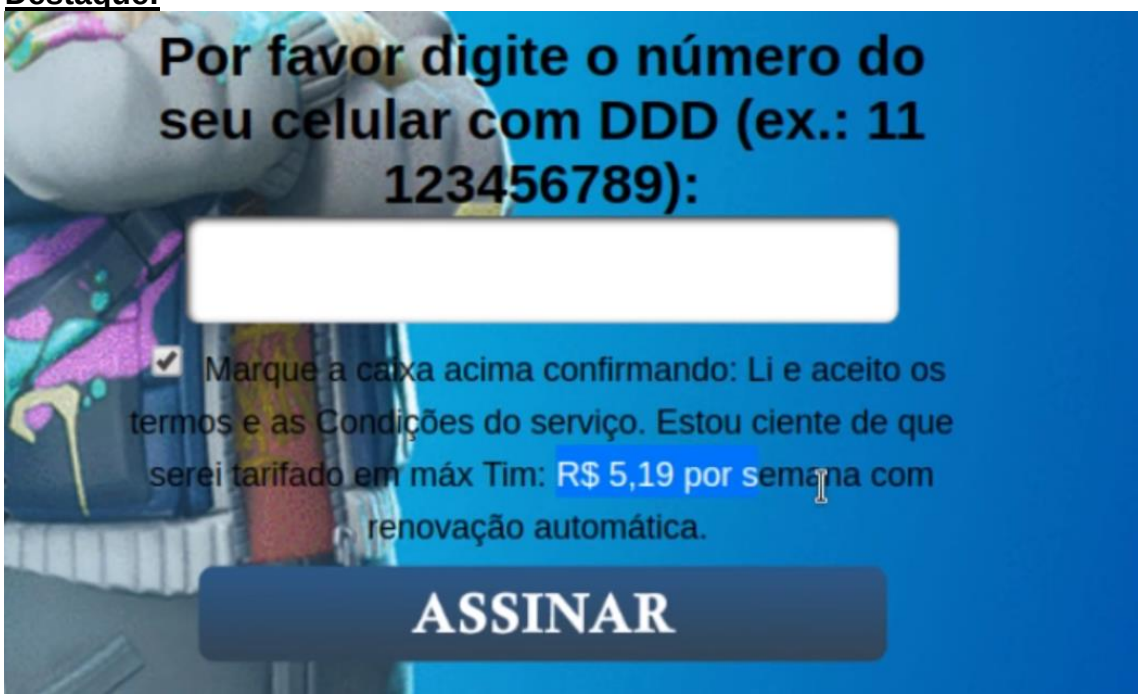
próprias lojas, o que inclui a verificação por malware, não trazendo, portanto, risco àqueles que baixaram tais aplicativos.

16. Outras atividades, quando o link era acessado por um computador (desktop), incluíam a adesão de planos de assinatura de mensagens de textos com temáticas de jogos e o preenchimento de pesquisas de opinião.

17. Estas atividades, porém, eram exibidas em sites de terceiros, fora da temática explorada pelo golpista (de sorteios de Iphones) e deixavam claro ao usuário a proposta de adquirir um plano de assinatura de mensagens. Vejamos:



Destaque:



18. Tais visitas e cadastros, nestes sites, também recompensam o golpista/invasor, e estes valores são pagos por esta rede de anúncios norte-americana, que remunera cada clique/download, todavia, o criminoso utiliza-se de links postados no Instagram dos famosos que ele invade, para ter estes cliques (de maneira ilícita). Reitera-se que a empresa responsável por esse serviço de rede de anúncios e pagamento por cliques, não é ilícita.

19. O serviço é permitido e legal, todavia, o criminoso deturpou o serviço para conseguir ganhar dinheiro pelos cliques nos links, e tarefas realizadas, que ele divulga com as invasões, obtendo assim, mais acessos e mais ganhos.

20. Ao final, após concluir as atividades exigidas no site, o usuário que acreditava que iria ganhar o Iphone, é redirecionado novamente ao início das atividades, tendo que realizar novas tarefas, permanecendo, aquele que deseja ganhar o Iphone, neste ciclo sem fim, sendo que, cada vez que o usuário/vítima refizer alguma das atividades, o invasor/golpista será novamente remunerado.

CONCLUSÃO

21. **Concluo que os mais de 600 mil seguidores, que acessaram o link postado pelo criminoso no Instagram @Cleo, não tiveram seus dispositivos expostos à riscos, invasões ou coleta de dados.**

22. **Reitera-se que, se fizeram algum download de aplicativo apontado no site, estes vieram de meios de distribuição oficiais e foram previamente revisados e aprovados pelas plataformas oficiais, e se clicaram em algum dos links (quando o acesso era realizado no computador) apenas receberam propostas publicitárias.**

23. **Em minha análise deste link (página), não encontrei a exploração de vulnerabilidades ou o oferecimento de *malware* aos dispositivos dos visitantes, vale dizer, não constatei risco de instalação de vírus (nos dispositivos e computadores dos usuários/vítimas), quando do acesso dos links postados pelo invasor/criminoso.**

24. O modelo de monetização por clique usado pelo invasor não é inédito, podendo ser encontrado em outros golpes similares na Internet, como oferecimento de download de filmes grátis, jogos grátis e etc., utilizando-se, inclusive, da mesma rede de distribuição de anúncios.

25. **Por fim, penso que o interesse do criminoso que invadiu o Instagram @Cleo e postou um link de suposta doação de Iphones, era de que as vítimas (seguidores) clicassem neste link, sendo direcionadas a uma página, para que realizassem alguma das atividades/downloads/verificações/tarefas ali solicitadas. Com os**

cliques e a realização destes procedimentos pelos usuários enganados, o criminoso era remunerado.

**Gabriel Pato – Especialista em Segurança da Informação, Consultor e Analista de vulnerabilidades em sistemas de empresas no Brasil e no exterior. Integra a Lista de Honra da Microsoft e a Lista de Agradecimentos da MasterCard e Facebook pelas fragilidades que encontrou nos sistemas destas empresas. Mantém o maior canal de tecnologia e segurança da Informação do Youtube/Brasil, com mais de 445 mil inscritos.*