



**MJSP - POLÍCIA FEDERAL
DIRETORIA DE INTELIGÊNCIA POLICIAL
COORDENAÇÃO-GERAL DE INTELIGÊNCIA
Divisão de Contraineligência Policial**

**À SUA EXCELÊNCIA O SR. JUIZ FEDERAL DA 10ª VARA DA SEÇÃO JUDICIÁRIA DO
DISTRITO FEDERAL**

**Referência: Inquérito Policial nº 02/2019-7/DICINT/CGI/DIP/PF
Processo PJE nº 1015706-59.2019.4.01.3400**

RELATÓRIO

1 - OBJETO DO INQUÉRITO

O presente Inquérito Policial foi inicialmente instaurado com o objetivo de apurar a aparente clonagem do telefone celular nº (041)99944-4140/TIM, que era utilizado pelo Sr. Ministro de Estado da Justiça e da Segurança Pública, Dr. Sérgio Moro, bem como identificar os autores da possível invasão realizada na conta do aplicativo de comunicação Telegram vinculada ao referido terminal móvel.

Conforme o ofício de requisição nº 1159/2019/GM (fls. 03/04), no dia 04 de junho de 2019, por volta das 18 horas, o Ministro Sérgio Moro recebeu três ligações cujo número chamador era o seu próprio terminal celular (041-99944-4140), tendo atendido a primeira chamada, que não foi completada, e deixado de atender as outras duas ligações. Narrou o Ministro que, logo em seguida, recebeu a mensagem de um jornalista informando que alguém teria ingressado no Telegram a partir de seu número, sendo que até aquele momento referido aplicativo não estava ativo em seu aparelho celular.

No Laudo Pericial nº 1195/2019-INC/DITEC/PF (Apenso II), os Peritos Criminais Federais relatam que o Ministro de Estado da Justiça e da Segurança Pública também teria recebido chamadas de números atípicos, como "000041", além de mensagens referentes

1





MJSP - POLÍCIA FEDERAL
DIRETORIA DE INTELIGÊNCIA POLICIAL
COORDENAÇÃO-GERAL DE INTELIGÊNCIA
Divisão de Contraineligência Policial

ao código de verificação do aplicativo Telegram e a protocolos da operadora TIM confirmando a adesão a serviços não solicitados.

Às fls. 21/36 foram juntadas as informações enviadas à Polícia Federal com o relato das invasões dos aparelhos celulares (*smartphones*) do Desembargador Federal Abel Gomes (TRF 2ª Região) e do Juiz Federal Flávio Lucas (18ª Vara Federal do Rio de Janeiro). Por sua vez, às fls. 37/39 consta a informação a respeito das invasões dos dispositivos de telefonia do Chefe da Delegacia da Polícia Federal de Campinas, DPF Edson Geraldo de Souza, e do Chefe do Núcleo de Inteligência daquela unidade, DPF Flávio Vieitez Reis. Tendo em vista a similitude dos fatos que estavam sendo narrados, avaliou-se que todos os ataques poderiam ter a mesma origem, tendo sido utilizada a estratégia de apurar todos esses fatos no mesmo Inquérito Policial.

Posteriormente, foram ainda noticiados à Polícia Federal os seguintes ataques a telefones celulares de autoridades públicas: i) Delegado de Polícia Federal Rafael Fernandes, lotado na SR/PF/SP (Apenso I); ii) Deputada Federal Joice Hasselmann (fl. 98); iii) Ministro de Estado da Economia Paulo Guedes (fls. 188/194); iv) Conselheiro do Conselho Nacional do Ministério Público (CNMP) Marcelo Weitzel (fls. 462/480); e v) Conselheiro do CNMP Silvio Roberto de Oliveira de Amorim Júnior (518/520).

Entretanto, verificou-se que o objeto do presente Inquérito Policial seria muito mais amplo do que aquele idealizado no início das investigações. As apurações realizadas levaram à identificação de um grupo criminoso especializado na prática de várias modalidades de crimes cibernéticos, cujos integrantes participaram, com níveis diferentes de atuação, dos ataques a milhares de telefones celulares e da interceptação de comunicações de centenas de pessoas.

A amplitude das ações criminosas praticadas dificulta até mesmo a qualificação de todas as vítimas do grupo investigado. Conforme o Laudo de Perícia de Informática nº 580/2019-UTEC/DPF/UDI/MG, foi verificado que os clientes ID 34221, ID 16737,





MJSP - POLÍCIA FEDERAL
DIRETORIA DE INTELIGÊNCIA POLICIAL
COORDENAÇÃO-GERAL DE INTELIGÊNCIA
Divisão de Contraineligência Policial

ID 69916 e ID 42680 cadastrados na BRVOZ, uma das operadoras¹ de telefonia de voz sobre IP utilizada por WALTER DELAGATTI NETO, GUSTAVO HENRIQUE ELIAS SANTOS e THIAGO ELIEZER MARTINS SANTOS como plataforma para as invasões, realizaram **7699** ligações em que o número de origem era igual ao número de destino, característica principal dos ataques, alcançando o total de **1727** números telefônicos de vítimas diferentes. Ressalte-se que ainda estão sendo realizadas diligências visando a identificação de todas as vítimas das invasões de dispositivos telemáticos.

Entretanto, o Laudo nº 1195/2019-INC/DITEC/PF (Apenso II dos autos) listou diversos números telefônicos de autoridades, jornalistas e pessoas públicas que tiveram ligações com número de origem igual ao número de destino, conforme registrado no sistema da empresa BRVOZ (MEGAVOIP), o que indica terem sido alvos dos ataques:

	NÚMERO	CONTATO	CONTA MEGAVOIP	LIGAÇÕES
1	619928xxxxx	Rodrigo Janot Monteiro de Barros	34221	76
2	419840xxxxx	Deltan Martinazzo Dallagnol	34221	37
4	119888xxxxx	Thamea Danelon Valiengo	34221	22
5	119633xxxxx	Orlando Martello Junior	34221	21
6	119833xxxxx	Moraes Dr. Alexandre de	34221	13
7	619954xxxxx	Nicolao Dino de Castro e Costa Neto	34221	13
8	619955xxxxx	Claudio Dantas	34221	12
9	619811xxxxx	João Otávio de Noronha	34221	10
10	619988xxxxx	Dep. Eduardo Bolsonaro	34221	10
11	619992xxxxx	Dep. Rodrigo Maia	34221	10
12	219926xxxxx	José Augusto Simões Vagos	34221	10
13	119632xxxxx	Márcio Barra Lima	34221	10

¹ Foi verificado que a empresa SETETEL, que presta serviços de telefonia de VoIP, foi também utilizada nos ataques.

(Assinatura manuscrita)





MJSP - POLÍCIA FEDERAL
DIRETORIA DE INTELIGÊNCIA POLICIAL
COORDENAÇÃO-GERAL DE INTELIGÊNCIA
Divisão de Contraineligência Policial

14	219920 xxxxx	Paulo Gomes Ferreira Filho	34221	10
15	419982 xxxxx	Delegado Franscischini	34221	9
16	619811 xxxxx	Paulo chefe gan Senador Davi	34221	9
17	419990 xxxxx	Andre Duszezak Jf	34221	9
18	419884 xxxxx	Roberson Mpf	34221	9
19	619927 xxxxx	Raquel Elias Ferreira Dodge	34221	9
20	139912 xxxxx	Thiago Lacerda Nobre	34221	9
21	419965 xxxxx	Dep. Felipe Franscischini	34221	8
22	169928 xxxxx	DPF Edson (Chefe da DPF/CAS/SP)	34221	8
23	119928 xxxxx	Dep. Luiz Philippe O. Bragança	69916	8
24	519924 xxxxx	Januario Paludo	34221	8
25	619916 xxxxx	Wagner Rosário	34221	7
26	619811 xxxxx	Luis Felipe Salomão	34221	7
27	619918 xxxxx	Dep. Gleisi Hoffmann	34221	7
28	619999 xxxxx	Dep. Paulo Teixeira	34221	7
29	119757 xxxxx	Lider Joice Hasselman	34221	7
30	419918 xxxxx	Deltan	34221	7
31	619995 xxxxx	Eduardo Bolsonaro	34221	7
32	219951 xxxxx	Flavio Bolsonaro	34221	7
33	219999 xxxxx	Presidente Bolsonaro Reservado	34221	7
34	619912 xxxxx	Presidente Bolsonaro Telefone Funcional	34221	7
35	119767 xxxxx	Cel Hideo	34221	6
36	169961 xxxxx	Dep. Baleia Rossi	34221	6
37	719864xxxxxx	Dr. Tiago Ayres (ADV PSL/Bolsonaro)	34221	6






MJSP - POLÍCIA FEDERAL
DIRETORIA DE INTELIGÊNCIA POLICIAL
COORDENAÇÃO-GERAL DE INTELIGÊNCIA
Divisão de Contraineligência Policial

38	859880 xxxxx	Gomes Sen Cid	34221	6
39	219741 xxxxx	Marisa Varotto Ferrari	34221	6
40	119819 xxxxx	Dep. Kim Kataguirí	34221	5
41	21995 xxxxx	Abel Des	34221	5
42	219889 xxxxx	Eduardo El Hage MPFRJ Força Tarefa	34221	5
43	319923 xxxxx	Júlio Carlos Motta Noronha	34221	5
44	119633 xxxxx	Isabel Cristina Groba Vieira	34221	5
45	119894 xxxxx	Karen Louise Jeanette Kahn	34221	5
46	619929 xxxxx	Luiza Cristina Fonseca Frischeisen	34221	5
47	119819 xxxxx	DGP SP Youssef	34221	4
48	419994 xxxxx	Ministro Sergio Moro	34221	4
50	119937 xxxxx	Carlos Alexandre da Costa Secretario do Guedes	34221	4
51	419915 xxxxx	Gabriela Jfs	34221	4
52	119834 xxxxx	DPF Rafael Fernandes Souza Dantas	34221	4
53	119762 xxxxx	Andrey Borges de Mendonça	34221	4
54	119887 xxxxx	Eduardo Botao Pelella	34221	4
55	419841 xxxxx	Flávia Cecília Maceno Blanco / Chefe de Gabinete	34221	3
56	119962 xxxxx	Abraham Bragança de V. Weintraub	34221	3
57	119928 xxxxx	Dep. Luiz Philippe O. Bragança	42680	3
58	219890 xxxxx	Eduardo Paes	34221	3
59	119727 xxxxx	GE Lamoso AJO Gov SP	34221	3
60	219859 xxxxx	Pezao Gov Rio	34221	3





MJSP - POLÍCIA FEDERAL
DIRETORIA DE INTELIGÊNCIA POLICIAL
COORDENAÇÃO-GERAL DE INTELIGÊNCIA
Divisão de Contraineligência Policial

61	219880 xxxxx	Flávio Lucas	34221	3
62	619937 xxxxx	Igor Gadelha Crusoe	34221	3
63	219860 xxxxx	Pedro Bial	34221	3
64	169927 xxxxx	André Luiz Moraes de Menezes	34221	3
65	619957 xxxxx	Danilo Pinheiro Dias	34221	3
66	519933 xxxxx	Douglas Fischer	34221	3
67	169938 xxxxx	Rudson Coutinho da Silva	34221	3
68		Abilio Diniz	34221	2
69	619811 xxxxx	Alcolumbre Sem Davi	34221	2
72	169970 xxxxx	Marcelo Barbieri (SRI/SEGOV)	34221	2
73	319880xxxxx	Athayde Ribeiro Costa	34221	2
74	219937xxxxx	General Braga Neto	34221	2
75	619819xxxxx	MRE Filipe	69916	2
76	119820xxxxx	Mario Carvalho Fsp	34221	2
77	219978xxxxx	Paulo Guedes	34221	2
78	219998xxxxx	Reis Friede Des Trf2	34221	2
79	419980xxxxx	Rosangela	34221	2
80	439880xxxxx	Diogo Castor de Mattos	34221	2
81	169919xxxxx	Gabriel da Rocha	34221	2
82	419881xxxxx	Paulo Roberto Galvão de Carvalho	34221	2
83	619953xxxxx	Silvio Amorim	34221	2
85	219998xxxxx	Oliveira Sen Arolde	16894	1
86	119814xxxxx	Sara Fernanda Leme Bandeira	34221	1
87	219870xxxxx	Marcelo Bretas	34221	1
88	619914xxxxx	Oswaldo Jose Barbosa Silva	34221	1

Entretanto, a listagem incluída no Laudo nº 1195/2019 não é exaustiva, mas apenas uma amostra das inúmeras vítimas dos ataques elaborada pelos Peritos da Polícia

6





MJSP - POLÍCIA FEDERAL
DIRETORIA DE INTELIGÊNCIA POLICIAL
COORDENAÇÃO-GERAL DE INTELIGÊNCIA
Divisão de Contraineligência Policial

61	219880 xxxxx	Flávio Lucas	34221	3
62	619937 xxxxx	Igor Gadelha Crusoe	34221	3
63	219860 xxxxx	Pedro Bial	34221	3
64	169927 xxxxx	André Luiz Moraes de Menezes	34221	3
65	619957 xxxxx	Danilo Pinheiro Dias	34221	3
66	519933 xxxxx	Douglas Fischer	34221	3
67	169938 xxxxx	Rudson Coutinho da Silva	34221	3
68	119998xxxxxx	Abilio Diniz	34221	2
69	619811 xxxxx	Alcolumbre Sem Davi	34221	2
72	169970 xxxxx	Marcelo Barbieri (SRI/SEGOV)	34221	2
73	319880xxxxxx	Athayde Ribeiro Costa	34221	2
74	219937xxxxxx	General Braga Neto	34221	2
75	619819xxxxxx	MRE Filipe	69916	2
76	119820xxxxxx	Mario Carvalho Fsp	34221	2
77	219978xxxxxx	Paulo Guedes	34221	2
78	219998xxxxxx	Reis Friede Des Trf2	34221	2
79	419980xxxxxx	Rosangela	34221	2
80	439880xxxxxx	Diogo Castor de Mattos	34221	2
81	169919xxxxxx	Gabriel da Rocha	34221	2
82	419881xxxxxx	Paulo Roberto Galvão de Carvalho	34221	2
83	619953xxxxxx	Silvio Amorim	34221	2
85	219998xxxxxx	Oliveira Sen Arolde	16894	1
86	119814xxxxxx	Sara Fernanda Leme Bandeira	34221	1
87	219870xxxxxx	Marcelo Bretas	34221	1
88	619914xxxxxx	Oswaldo Jose Barbosa Silva	34221	1

Entretanto, a listagem incluída no Laudo nº 1195/2019 não é exaustiva, mas apenas uma amostra das inúmeras vítimas dos ataques elaborada pelos Peritos da Polícia

6





MJSP - POLÍCIA FEDERAL
DIRETORIA DE INTELIGÊNCIA POLICIAL
COORDENAÇÃO-GERAL DE INTELIGÊNCIA
Divisão de Contraineligência Policial

Federal a partir da agenda de contatos armazenada no aparelho celular do Ministro Sérgio Moro², bem como da relação de telefones funcionais de membros do MPF fornecida pela Procuradoria-Geral da República, sendo que diversas outras vítimas foram sendo identificadas ao longo das investigações.

Assim, dentre as vítimas dos ataques se encontram autoridades públicas dos três poderes da República e de diferentes esferas da administração, como Ministros de Estado, Senadores, Deputados Federais, Ministros da Suprema Corte, Ministros do Superior Tribunal de Justiça, Desembargadores, Juizes Federais e Estaduais, Procuradores da República, dentre os quais dois ex-Procuradores-Gerais da República, Delegados de Polícia Federal, Delegados e investigadores da Polícia Civil do Estado de São Paulo e membros do Ministério Público do Estado de São Paulo.

A seleção dos alvos dos ataques indica, por sua vez, que um dos objetivos das ações seria causar obstáculos ou embaraçar investigações que visam organizações criminosas, tendo em vista que os autores do crime procuraram deliberadamente invadir contas do Telegram de membros do Ministério Público Federal que atuam na Força-Tarefa da Lava Jato no Estado do Paraná, divulgando para a imprensa informações sigilosas envolvendo investigações e processos criminais em curso.

Cada vítima pode ter sido alvo de dois tipos de ações que eram promovidas pelos investigados, que poderiam ocorrer simultaneamente: i) a extração das mensagens, documentos e agendas de contatos armazenados no aplicativo Telegram; e ii) o monitoramento em tempo real das mensagens que eram trocadas pelas vítimas com outros interlocutores, através da ativação de novas seções do aplicativo por meio do programa Telegram Desktop instalado no computador do atacante. Em algumas situações, também era realizada a ativação da conta no Telegram vinculada do telefone do alvo, caso o aplicativo não estivesse instalado ou

² O aparelho celular do Ministro Sérgio Moro foi apresentado e submetido a exame pericial pelo Instituto Nacional de Criminalística, conforme Laudo de Perícia Criminal Federal nº 1118/2019-INC/DITEC/PF (fls. 105/109).





MJSP - POLÍCIA FEDERAL
DIRETORIA DE INTELIGÊNCIA POLICIAL
COORDENAÇÃO-GERAL DE INTELIGÊNCIA
Divisão de Contraineligência Policial

não fosse utilizado, que passava a ser controlada pelo criminoso para enviar mensagens para terceiros em nome da vítima.

Por sua vez, verifica-se que a expertise inicial dos integrantes do grupo consistia na prática de fraudes bancárias eletrônicas, a clonagem de cartões de crédito e furtos virtuais de contas bancárias. Para a execução de tais crimes eram empregadas diversas técnicas distintas, tais como a falsificação de documentos, o extravio de cartões bancários, a introdução de *softwares* maliciosos e a utilização de engenharia social, termo utilizado para descrever o uso da persuasão, muitas vezes abusando da ingenuidade ou confiança do usuário, para obter informações que podem ser utilizadas para ter acesso não autorizado a sistemas de computadores.

Do mesmo modo, percebe-se que a metodologia utilizada para efetuar a invasão das contas do Telegram de autoridades públicas foi inicialmente desenvolvida justamente para a obtenção de dados de vítimas de fraudes bancárias, estelionatos virtuais e outros crimes cibernéticos, tais como gerentes de instituições financeiras e seus clientes. Embora o foco principal do presente relatório seja as invasões de dispositivos informáticos e a interceptação de comunicações de autoridades públicas, bem como a utilização de referidas mensagens para causar embaraços a investigação de infração penal envolvendo organizações criminosas, serão mencionadas algumas das fraudes bancárias já identificadas, bem como ações voltadas à ocultação e dissimulação da origem ilícita dos recursos obtidos movimentados pelo grupo.

2 – O MECANISMO UTILIZADO NOS ATAQUES A CONTAS DO APLICATIVO TELEGRAM

Foi realizada a perícia no aparelho celular nº (041) 99944-4140/TIM, utilizado pelo Ministro Sérgio Moro, para apurar um eventual acesso indevido ao dispositivo, conforme procedimentos e exames descritos no Laudo nº 1118/2019-INC/DITEC/PF (fls. 105/109). Entretanto, segundo as análises da DITEC/PF, não foram encontradas no aparelho celular quaisquer evidências acerca da exploração de possíveis vulnerabilidades que permitisse o

8





MJSP - POLÍCIA FEDERAL
DIRETORIA DE INTELIGÊNCIA POLICIAL
COORDENAÇÃO-GERAL DE INTELIGÊNCIA
Divisão de Contraineligência Policial

acesso malicioso do dispositivo. Na realização da perícia foram extraídos os registros de mensagens e telefonemas recebidos pelo Ministro Sérgio Moro no dia 04/06/2019, que foram relacionados na tabela abaixo:

Data e hora	Tipo	Número de origem	Duração (s)	Detalhes/Conteúdo
04.06.2019 17:40:32	SMS recebido	29095	-	Telegram code: 18366 You can also tap on this link to log in: https://t.me/login/18366
04.06.2019 17:41:47	SMS recebido	28060	-	Telegram code: 18366 You can also tap on this link to log in: https://t.me/login/18366
04.06.2019 17:45:30	Chamada recebida	041999444140	6	
04.06.2019 17:45:34	Chamada recebida	000041	0	
04.06.2019 17:45:48	Chamada recebida	041999444140	0	
04.06.2019 17:46:07	Chamada recebida	041999444140	0	
04.06.2019 17:46:16	SMS recebido	100	-	TIM RECADO: Você recebeu um novo recado. Para saber mais sobre como ouvir, ligue *100.
04.06.2019 17:46:43	Chamada recebida	041999444140	0	
04.06.2019 17:47:07	SMS recebido	4198	-	Protocolo 2019630534419 aberto em 04-06-2019 as 17:47:06, referente a sua solicitação concluída através de nosso atendimento.
04.06.2019 17:47:12	SMS recebido	100	-	Você assinou o TIM Recado Backup Mes e além de ouvir recados a vontade vai receber as mensagens por SMS! Aproveite! R\$6,09 por mes. Para cancelar ligue *100

Imagem da Tabela 2 do Laudo nº 1195/2019-INC/DITEC/PF.

Conforme Laudo nº 1195/2019-INC/DITEC/PF (Apenso II), após a análise dos registros de ligações e mensagens ocorridas no período próximo à possível tentativa de acesso não autorizado do celular número (41) 99944-4140, os Peritos Criminais Federais puderam chegar às seguintes conclusões:

- i) Antes de receber qualquer ligação, o telefone em questão recebeu duas mensagens SMS informando um código de verificação do aplicativo Telegram;





MJSP - POLÍCIA FEDERAL
DIRETORIA DE INTELIGÊNCIA POLICIAL
COORDENAÇÃO-GERAL DE INTELIGÊNCIA
Divisão de Contraineligência Policial

ii) A primeira das chamadas cujo número de origem é o mesmo do de destino foi transmitida para o telefone celular questionado e atendida (duração entre 6 e 7 segundos);

iii) O telefone não registrou o recebimento da chamada cuja origem é o número 17147073350, tendo tal ligação sido encaminhada para a caixa de mensagens do celular. A partir de testes realizados pelos peritos, verificou-se o número 17147073350 é utilizado pelo aplicativo para informar o código de validação por meio de mensagem de voz. Provavelmente o redirecionamento da chamada se deu porque a linha telefônica do celular nº (41) 99944-4140 estava ocupada pela ligação recebida do próprio número. Ao ser redirecionado para a caixa de mensagens, o código informado por mensagem de voz teria sido gravado na caixa de mensagens, o que é evidenciado pela mensagem SMS com data de recebimento às 17:46:16 do dia 04/06/2019;

iv) As três chamadas com número de origem igual ao número de destino, apesar de terem sido registradas no celular nº (41) 99944-4140, não foram atendidas, mas acabaram sendo direcionadas para a caixa de mensagens, e tiveram duração de 7, 8 e 58 segundos, respectivamente.

Peritos Criminais Federais também elaboraram Informação detalhando as tentativas de acesso não autorizado ao aplicativo dos Delegados de Polícia Federal que atuam no Estado de São Paulo, quando foram reunidas as capturas de tela (*prints*) com os dados de seções do aplicativo não reconhecidas pelos seus usuários, conforme figuras abaixo:





MJSP - POLÍCIA FEDERAL
DIRETORIA DE INTELIGÊNCIA POLICIAL
COORDENAÇÃO-GERAL DE INTELIGÊNCIA
Divisão de Contraineligência Policial



Pela imagem acima, foi possível observar que as sessões atípicas identificadas estariam presentes em um "iPhone XS Max, iOS 12.3.1" e em um "PC, Windows 10". Por sua vez, os endereços IP correspondentes foram identificados como provenientes de serviços VPN, que ocultam o real utilizador da internet. Assim, com base nas informações reunidas pelos Peritos Criminais da Polícia Federal, determinou-se o mecanismo empregado pelos criminosos, conforme as subseções III.3.1 a III.3.7 do Laudo nº 1195/2019-INC/DITEC/PF (Apenso II), que serão detalhadas a seguir:

Em sistemas de telefonia, a "Caixa de Mensagens" é um recurso utilizado para deixar mensagens de voz para o destinatário da ligação quando este não pode atender. Tais sistemas têm funcionamento semelhante às antigas "Secretárias Eletrônicas". Quando este recurso está ativo, caso o telefone de destino da chamada não esteja registrado na rede (desligado ou fora da área de cobertura) ou esteja ocupado em outra ligação, é dada a opção para quem liga de gravar uma mensagem, que pode ser posteriormente ouvida pelo destinatário.

Para o destinatário ouvir as mensagens gravadas em sua caixa de mensagens o usuário deve ligar para um número específico do serviço, que varia de operadora





MJSP - POLÍCIA FEDERAL
DIRETORIA DE INTELIGÊNCIA POLICIAL
COORDENAÇÃO-GERAL DE INTELIGÊNCIA
Divisão de Contraineligência Policial

para operadora (números comuns no Brasil são o *100 ou *555). Ao receber a ligação, a operadora verifica o número de origem da chamada e seleciona a caixa de mensagens relativas àquele número. Algumas operadoras disponibilizam outros números de acesso alternativos, como, por exemplo, para quando o usuário está no exterior ou pretenda acessar sua caixa de mensagens ligando de outro número que não seja o seu próprio. Neste caso, em geral, é necessária uma senha para que o acesso seja concedido.

Uma outra forma comumente implementada pelas operadoras de telefonia para acesso direto à caixa de mensagens é a ligação para o próprio número. Ou seja, se um indivíduo deseja ouvir as mensagens gravadas em sua caixa de mensagens, ele liga para seu próprio número e a operadora desvia a ligação para a caixa de mensagens. Assim, os peritos realizaram testes utilizando seus telefones celulares pessoais, de diversas operadoras, e conseguiram, geralmente, acesso irrestrito às suas caixas de mensagens utilizando este procedimento.

Os Peritos da Polícia Federal então verificaram que era possível que o número de origem de uma ligação fosse alterado para um número falso, ou até mesmo para números válidos registrados para outros usuários. Foram encontrados sítios na internet ou aplicativos para celulares que alteram o número de origem da ligação (*spoofing*), tais como o "Spoof My Phone" e o "Spoofcard", permitindo que sejam realizadas ligações configurando números forjados como a origem das chamadas. Do mesmo modo, tais alterações de números de origem de chamadas ainda é possível através de operadoras de voz sobre IP (VoIP), uma vez que muitas empresas oferecem a possibilidade da configuração livre do número de origem das ligações realizadas por seus sistemas.

Assim, utilizando o método de forjar o número de origem da chamada (seja por uso de aplicativos ou por meio de operadoras de telefonia VoIP que possibilitem alterar o número de origem), seria possível a acessar uma caixa de mensagem alheia, realizando uma ligação para o número de destino e configurando como origem da ligação esse mesmo número. Ao efetuar este tipo de chamada, a operadora de telefonia celular considera que seria uma





MJSP - POLÍCIA FEDERAL
DIRETORIA DE INTELIGÊNCIA POLICIAL
COORDENAÇÃO-GERAL DE INTELIGÊNCIA
Divisão de Contrainteligência Policial

ligação para o próprio número e a redireciona para a caixa de mensagens, concedendo acesso total ao serviço. Desta forma, seria possível ouvir as mensagens gravadas, apagar mensagens, contratar serviços relacionados, entre outras ações.

Por sua vez, também foi constatado que o aplicativo de mensagens Telegram utiliza o telefone do usuário como forma de identificá-lo, podendo a validação do número de telefone vinculado ocorrer através de mensagem de voz. Nesses casos, o usuário recebe uma ligação telefônica com o código de verificação informado por uma gravação e, caso não atenda a chamada, por estar desligado ou ocupado em outra chamada, a ligação do aplicativo Telegram é direcionada para a caixa de mensagens e o código gravado como uma mensagem de voz.

Assim, segundo os Peritos da Polícia Federal, um atacante poderia instalar o aplicativo Telegram em outro dispositivo e informar como identificação o número de telefone da vítima. Neste momento, o aplicativo envia o código de verificação, inicialmente para as outras sessões abertas e, posteriormente, via mensagem de voz, ou seja, por meio de uma ligação telefônica para o número vinculado. No mesmo instante, o atacante pode realizar diversas ligações para o número da vítima, de forma a ocupar sua linha e forçar que a ligação com o código de verificação do Telegram caia na caixa de mensagens da vítima e seja ali gravada como recado.

Em seguida, o atacante ainda poderia utilizar o recurso de acesso indevido à caixa de mensagens da vítima realizando uma ligação para o telefone atacado com o número de origem da chamada adulterado, configurando o número de destino como sendo o utilizado pela vítima. Acessando a caixa postal do alvo, o atacante poderia então ouvir a mensagem de voz com o código de verificação, conseguindo, desta forma, o acesso ao aplicativo Telegram, habilitando-o em outro dispositivo como se fosse da própria vítima.

O aplicativo Telegram armazena todas as mensagens dos usuários em seus servidores, possibilitando ainda que cada usuário possa ter várias sessões abertas simultaneamente. Assim, uma vez que o atacante consiga o controle das sessões das contas de





MJSP - POLÍCIA FEDERAL
DIRETORIA DE INTELIGÊNCIA POLICIAL
COORDENAÇÃO-GERAL DE INTELIGÊNCIA
Divisão de Contraineligência Policial

terceiros no Telegram, ele poderá ler todas as mensagens trocadas pelo aplicativo em tempo real, bem como as mensagens antigas que estejam armazenadas no servidor do Telegram, além de arquivos de mídia e documentos enviados e recebidos.

De acordo com a documentação do Telegram, apenas mensagens selecionadas com a função *Time-bomb* não permanecem salvas no *backup* do servidor. Dessa forma, é possível ter acesso a mensagens antigas e atuais da vítima, permitindo inclusive o download das mensagens para uma análise posterior.

Além disso, também foi observado pelo Peritos Criminais que cada chamada realizada para ouvir integralmente uma mensagem de voz do aplicativo Telegram com o código de verificação tinha duração mínima de 25 segundos. Este tempo, entretanto, não leva em consideração o tempo necessário para apagar a mensagem depois de ouvida, podendo também variar de acordo com a operadora.

Os Peritos Criminais da Polícia Federal, ao elaborarem o Laudo nº 1195/2019-INC/DITEC/PF (Apenso II), realizaram diversas reproduções simuladas das ações maliciosas visando reproduzir e validar os ataques em um ambiente de laboratório, conforme descrito no item III.3.8. Segundo os exames, os testes foram bem sucedidos para linhas das operadoras Claro, TIM e Vivo, que eram a que estavam no escopo dos teste.

Para os testes referentes à operadora TIM, que era a telefônica utilizada na linha do Ministro Sérgio Moro, foi possível também ativar o serviço de caixa de mensagem, denominado pela operadora de "TIM Recado Backup", apenas digitando o número "1" duas vezes, seguindo instruções do menu. Após a ativação do serviço foi possível ouvir a mensagem com o código de validação do aplicativo Telegram, que poderia ser também apagada. Verificou-se que após a ativação do serviço foram recebidas duas mensagens SMS da operadora TIM, que eram bastante semelhante àquelas recebidas pelo telefone do Ministro, uma com um número de protocolo e a segunda avisando da ativação do serviço "Tim Recado Backup".





MJSP - POLÍCIA FEDERAL
DIRETORIA DE INTELIGÊNCIA POLICIAL
COORDENAÇÃO-GERAL DE INTELIGÊNCIA
Divisão de Contraineligência Policial

Ressalte-se, por fim, que após a deflagração da Operação Spoofing a Agência Nacional de Telecomunicações (Anatel) determinou que as operadoras de telefonia corrigissem a brecha na rede de telefonia que permitiu a invasão dos celulares de centenas de autoridades do país. De acordo com a determinação da Anatel, agora não é mais possível acessar a caixa postal ligando para o seu próprio número, recurso que, embora bloqueado, não era considerada uma falha, mas um padrão da rede das operadoras, também utilizado em outros países. A mudança deve valer tanto para empresas convencionais, celulares e de VoIP, e vem como forma de bloquear a prática do *spoofing*, método usado pelos investigados em suas ações criminosas.

Do mesmo modo, a Anatel também teria orientado que as empresas de telefonia realizassem ações educativas para incentivar a adoção de senha para acessar a caixa postal, uma vez que boa parte dos usuários não altera a senha padrão de acesso à caixa postal, enviada pelas operadoras, o que facilita a ação de criminosos.

Além disso, a Anatel determinou que empresas de VoIP não poderão realizar chamadas a partir de números que não as pertençam, outro caminho que permitiu aos investigados utilizarem telefones que não eram deles para acessar caixas postais. A possibilidade de mascarar uma chamada com outro identificador ainda permanece disponível, mas apenas para sequências de uma mesma operadora e que não estejam já sendo usadas por terceiros.

Também fariam parte das medidas de bloqueio, ainda, os aplicativos e serviços internacionais que emulam chamadas de celulares ativos no Brasil. Para tanto, as operadoras teriam implementado filtros para ligações feitas do exterior, por meio da internet ou rede telefônica convencional, de forma a identificar tentativas irregulares de contatos que possam levar a ataques por essa metodologia.

Ainda em resposta à Operação Spoofing, a empresa que controla o Telegram também anunciou que estaria desativando o recebimento de códigos de ativação por meio de





MJSP - POLÍCIA FEDERAL
DIRETORIA DE INTELIGÊNCIA POLICIAL
COORDENAÇÃO-GERAL DE INTELIGÊNCIA
Divisão de Contrainteligência Policial

ligações telefônicas, a não ser que o usuário esteja usando o sistema de autenticação em duas etapas. A ausência desse dispositivo de segurança seria um aspecto fundamental que permitiu a invasão aos celulares do Ministro Sérgio Moro e demais autoridades, ainda que outras brechas no sistema telefônico brasileiro tenham também sido exploradas.

3 – A LINHA INVESTIGATIVA ADOTADA

A linha investigativa adotada inicialmente consistiu na verificação das rotas e interconexões das ligações efetuadas para o telefone do Ministro Sérgio Moro, notadamente das ligações que foram identificadas como originadas do próprio número telefônico que era utilizado pela vítima. Seguindo o rastreamento das ligações, observou-se que as chamadas utilizadas para realizar o acesso ao código enviado pelos servidores do aplicativo Telegram para a sincronização do serviço Telegram Web, relativo ao terminal celular nº 041 99944-4140, foi recebida na rede da operadora TIM a partir da operadora Embratel (CLARO BRASIL).

Por sua vez, com base nas informações recebidas da operadora Embratel (CLARO BRSIL), foi possível constatar que as chamadas com destino à rede da operadora TIM, que tinham como origem (número originador) e destino (número destinatário) o telefone 41 99944-4140, foram recebidas pela operadora EMBRATEL através da rota de interconexão com a operadora DATORA TELECOMUNICAÇÕES LTDA (Rota de Entrada 8885), conforme Informação nº 17/2019 – SOI/DICINT/CGI/DIP/PF.

Desta forma, realizou-se diligências na operadora de telefonia DATORA TELECOMUNICAÇÕES LTDA (DATORA) com o objetivo de levantar as informações sobre as chamadas que trafegaram na sua rede, com destino ao número 41 99944-4140, no período de 01/06/2019 a 10/06/2019. Em atendimento à requisição da Polícia Federal, realizada com suporte em ordem judicial, a operadora DATORA confirmou que transportou as chamadas destinadas ao número do Sr. Ministro Sérgio Moro, tendo informado, por sua vez, que as mesmas foram recebidas através da rota de interconexão, baseada em tecnologia VOIP, com o cliente abaixo identificado:





MJSP - POLÍCIA FEDERAL
DIRETORIA DE INTELIGÊNCIA POLICIAL
COORDENAÇÃO-GERAL DE INTELIGÊNCIA
Divisão de Contraineligência Policial

- Nome/Razão Social: DANILO BORGES DE BRITO – MEGAVOIP
- CNPJ 11.061.985/0001-81
- ENDEREÇO: RUA MARIA JUSTA 19 – PATOS DE MINAS – MG – CEP: 38701-078
- E-mail: megavoiptelecom@megavoiptelecom.com.br
- Telefone: +55 31 3014-9808
- IP de Origem: 108.61.154.194

Do mesmo modo, foi informado que os CDRs disponibilizados pela operadora DATORA, referentes às chamadas originadas da MEGAVOIP, foram extraídos do sistema de tarifação da empresa, e, portanto, não continham nenhuma outra informação que permitisse identificar o invasor:

megavoip_sip	5541999444140	5541999444140	BRAZIL	2_BR-41_Outras-Cell	6/4/2019 17:46	0:01:00	0.125
megavoip_sip	5541999444140	5541999444140	BRAZIL	2_BR-41_Outras-Cell	6/4/2019 17:46	0:00:30	0.0625
megavoip_sip	5541999444140	5541999444140	BRAZIL	2_BR-41_Outras-Cell	6/4/2019 17:45	0:00:30	0.0625
megavoip_sip	5541999444140	5541999444140	BRAZIL	2_BR-41_Outras-Cell	6/4/2019 17:45	0:00:30	0.0625

A operadora DATORA informou ainda que a rota de interconexão com o cliente MEGAVOIP é baseada na tecnologia VOIP (voz sobre IP), porém não armazenava os logs de sinalização das chamadas. O protocolo de sinalização utilizado era o SIP (*Session Initiation Protocol*), que se baseia no formato de requisições de texto e possui diversos campos onde são armazenadas informações que poderiam auxiliar na identificação do Invasor.

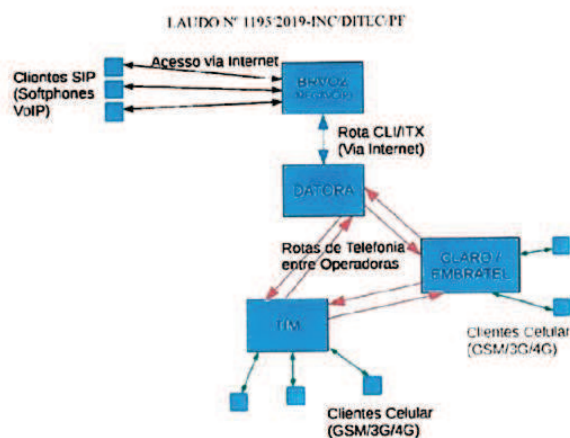
Por sua vez, foi verificado que a empresa MEGAVOIP, de propriedade de DANILO BORGES DE BRITO, possuía como nome fantasia a denominação **BRVOZ TELECOM**, com endereço comercial na Rua Maria Justa, 19, Lagoinha, Patos de Minas/MG, de acordo com a informação nº 20/2019 – SOI/DICINT/CGI/DIP/PF. A empresa DATORA também informou à Polícia Federal que a rota de interconexão com o cliente MEGAVOIP (BRVOZ) estava ativa, existindo várias chamadas que estariam trafegando naquele momento.





MJSP - POLÍCIA FEDERAL
DIRETORIA DE INTELIGÊNCIA POLICIAL
COORDENAÇÃO-GERAL DE INTELIGÊNCIA
Divisão de Contrainteligência Policial

A figura abaixo, extraída do Laudo nº 1195/2019-INC/DITEC/PF (Apenso II) ilustra as conexões entre operadoras e as possíveis rotas de ligações provenientes da empresa MEGAVOIP até o destino final (terminais de telefones celulares de diversas operadoras):



Através da análise de fontes abertas, foi constatado que a empresa BRVOZ disponibilizava serviços de telefonia baseados na tecnologia de Voz sobre IP (VOIP), conforme site hospedado no endereço <http://www.brvoz.com.br/>:



Assim, com base em tais informações, a Polícia Federal obteve ordem judicial para que a empresa BRVOZ fornecesse todas as informações necessárias para a





MJSP - POLÍCIA FEDERAL
DIRETORIA DE INTELIGÊNCIA POLICIAL
COORDENAÇÃO-GERAL DE INTELIGÊNCIA
Divisão de Contrainteligência Policial

investigação. Com isso foi permitido pela Justiça que os Peritos Criminais Federais tivessem acesso aos sistemas internos da empresa de telefonia de voz sob IP para o delineamento do quadro fático e a realização de perícia criminal, com o objetivo de identificar a autoria da invasão realizada na conta do aplicativo Telegram vinculada ao terminal celular nº 041 99944-4140/TIM, que era utilizado pelo Ministro Sérgio Moro, bem como de qualquer outro terminal telefônico que tivesse sido ilegalmente duplicado e invadido a partir da rede da MEGAVOIP (BRVOZ).

Do mesmo modo, foi determinado pelo juízo da 10ª Vara Criminal da Seção Judiciária do Distrito Federal que a empresa BRVOZ (MEGAVOIP) fornecesse à Polícia Federal todas as informações cadastrais, contratuais e bancárias dos clientes que realizaram ou receberam ligações por meio do telefone nº (041) 99944-4140, ou de quaisquer outros clientes que tivessem utilizado/duplicado indevidamente números telefônicos de terceiros, bem como os IPs de origem de todas as ligações suspeitas.

Visando identificar o modo de agir dos responsáveis pelos ataques às contas do Telegram de diversas autoridades públicas do país, e em cumprimento à determinação judicial expedida pela 10ª Vara Criminal Federal da Seção Judiciária do Distrito Federal, foi realizada diligência na sede da microempresa Megavoip Telecom (BRVOZ), quando o proprietário da firma individual MEGAVOIP disponibilizou-se a repassar todas as informações para a equipe de policiais designada, conforme Informação nº 006/2019 – SEPINF/DPER/INC/DITEC/PF (fls. 67/72).

4 – O FUNCIONAMENTO DO SISTEMA DA BRVOZ (MEGAVOIP)

A BRVOZ era uma microempresa que prestava serviços de telefonia de voz sobre IP (VOIP), permitindo que um cliente possa utilizar computadores, telefones convencionais ou celulares para fazer ligações de qualquer lugar do mundo, bastando estar conectado na internet. Segue abaixo o diagrama da solução da BRVOZ verificado em consulta ao site <http://www.brvoz.com.br/como-funciona/funcionamento> :





MJSP - POLÍCIA FEDERAL
DIRETORIA DE INTELIGÊNCIA POLICIAL
COORDENAÇÃO-GERAL DE INTELIGÊNCIA
Divisão de Contraineligência Policial



Para utilizar os serviços da BRVOZ cada cliente deve realizar o pagamento do valor do plano escolhido através de um boleto bancário a ser emitido pela empresa PagSeguro, após o preenchimento de alguns dados como *e-mail*, CEP, nome e número de celular. Ressalte-se que não havia qualquer mecanismo utilizado pela BRVOZ para verificar a autenticidade dos dados informados pelos clientes para a PagSeguro na emissão de cada boleto de pagamento.

Após a confirmação do pagamento, o cliente/usuário recebe um *e-mail* da BRVOZ, no endereço que foi informado no cadastro da empresa PagSeguro, solicitando informações para a criação de *login* no sistema da BRVOZ. Após o *login*, cada cliente/usuário recebe uma identificação única, denominada **ID (ID BRVOZ)**, no banco de dados da BRVOZ.

Ressalte-se, novamente, que o **ID** de cada cliente gerado nos cadastros da BRVOZ era alimentado com dados fornecidos pela PagSeguro e pelo próprio cliente através de mensagem de *e-mail*, tais como nome, CPF, telefone, endereço, os quais em sua maioria não eram verdadeiros, pois não havia nenhum mecanismo de checagem por parte da BRVOZ. Pode-se afirmar, assim, que somente os *e-mails* informados pelos clientes da BRVOZ nos cadastros **ID** suspeitos possuíam relevância para as investigações, pois este era o canal de comunicação utilizado entre a BRVOZ e seus usuários.

Por sua vez, também foi verificado que no sistema utilizado pela BRVOZ podiam ser concedidas permissões de funcionalidades distintas para a realização de ligações





MJSP - POLÍCIA FEDERAL
DIRETORIA DE INTELIGÊNCIA POLICIAL
COORDENAÇÃO-GERAL DE INTELIGÊNCIA
Divisão de Contraineligência Policial

por cada grupo de usuários/clientes, que são individualmente identificados por meio de número ID (ID BRVOZ). Dentre estas funcionalidades permitidas, destaca-se a função denominada IDENTIFICADOR DE CHAMADAS, que, caso fosse habilitada, fazia com que o usuário ID BRVOZ pudesse editar em cada ligação o número do telefone chamador.

Com a ativação da função IDENTIFICADOR DE CHAMADAS, as ligações realizadas pelo usuário da respectiva conta ID BRVOZ passavam a ser identificadas pelo receptor da ligação (número chamado) com o número informado pelo usuário (número chamador) no sistema da BRVOZ. Ou seja, utilizando a função IDENTIFICADOR DE CHAMADAS, o cliente/usuário da BRVOZ podia realizar ligações telefônicas simulando o número de qualquer terminal telefônico como origem das chamadas.

Do mesmo modo, conforme o Laudo nº 1195/2019-INC/DITEC/PF (Apenso II), foi esclarecido pelo proprietário da BRVOZ TELECOM que o sistema usado na empresa permitia que o cliente escolhesse livremente o número de origem das ligações, bastando que o usuário acessasse a área correspondente na página da empresa na internet. Foi esclarecido ainda que, para alguns clientes empresariais que contrataram o serviço de "0800" reverso, também chamado de "0800" via site ou "click-to-call", este tipo de ligação era realizado automaticamente: o cliente que contratava o serviço digitava um número de telefone para ser chamado, e o sistema fazia uma ligação com número de origem igual ao número de destino para este telefone.

Considerando que a ação maliciosa investigada somente seria possível mediante a realização de ligações com número de origem igual ao número de destino, os Peritos da Polícia Federal fizeram um levantamento na empresa BRVOZ para obtenção dos registros de todas as ligações desse tipo. A planilha com a listagem das contas que realizaram ligações com número de origem igual ao número de destino ($A = B$) foi copiada para mídia que está em apenso ao Laudo nº 1195/2019-INC/DITEC/PF (Apenso II), contendo colunas com a quantidade de ligações e a quantidade de números de telefones diferentes que foram alvo deste tipo de chamada por meio do sistema BRVOZ ("Ligacoes\Totaliza_Ligacoes_AB.xlsx").





MJSP - POLÍCIA FEDERAL
DIRETORIA DE INTELIGÊNCIA POLICIAL
COORDENAÇÃO-GERAL DE INTELIGÊNCIA
Divisão de Contrainteligência Policial

Conforme a Informação nº 006/2019-SEPINF/DPER/INC/DITEC/PF (fls. 67/72), dados fornecidos pela BRVOZ indicaram que todas as ligações suspeitas (com número de origem igual ao número de destino) para o número (41) 99944-4140 partiram da conta ID 34221. Assim, concluiu-se que o sistema da empresa BRVOZ foi utilizado para editar o número chamador e efetuar ligações para o mesmo número (número chamador = número chamado), sendo a plataforma que propiciou a invasão das contas do Telegram do Ministro Sérgio Moro, bem como de inúmeras outras vítimas de ataques semelhantes.

Conforme já mencionado, para ter o acesso às senhas do serviço Telegram Web os autores dos ataques criminosos conseguiram explorar uma vulnerabilidade comum a todas as operadoras de telefonia: as chamadas em que o número de origem é igual ao número de destino são direcionadas diretamente para a caixa postal sem necessidade de inserção de senha para acesso ao conteúdo das mensagens gravadas.

Entretanto, verificou-se que o sistema utilizado pela empresa BRVOZ (MEGA VOIP) gravava registros de *log* (informações gerais de eventos do sistema de aplicações em execução), dentre os quais endereços IP relacionados às atividades nas contas dos clientes (Informação nº 006/2019-SEPINF/DPER/INC/DITEC/PF - fls. 67/72). Assim, com a obtenção da listagem de endereços IP com a respectiva data e hora das atividades de cada conta de clientes da empresa de VoIP, foi possível à Polícia Federal identificar os responsáveis pela utilização do sistema da BRVOZ para realizar a invasão de contas do Telegram de diversas autoridades públicas do país, além de diversas outras vítimas, que tiveram suas comunicações interceptadas de forma ilegal.

Deve ser ressaltado, entretanto, que após a deflagração da Operação Spoofing foram encontrados registros nos computadores apreendidos do uso do programa de telefonia sobre IP (VoIP) denominado "Zoiper5", *software* que é utilizado para realizar e receber chamadas através da internet utilizando um computador pessoal, ao invés de usar um *hardware* dedicado. Por sua vez, em referido programa foi encontrada configurada, além das contas da





MJSP - POLÍCIA FEDERAL
DIRETORIA DE INTELIGÊNCIA POLICIAL
COORDENAÇÃO-GERAL DE INTELIGÊNCIA
Divisão de Contraineligência Policial

empresa BRVOZ, uma conta da empresa denominada SETETEL, indicando que os investigados também utilizariam outras plataformas de telefonia VoIP para realizar os ataques.

5 – A IDENTIFICAÇÃO DAS PESSOAS EM TORNO DOS FATOS

Após a análise do sistema e logs da BRVOZ foi possível apontar que todas as ligações efetuadas para o telefone nº (41) 99944-4140, utilizado pelo Sr. Ministro Sérgio Moro, partiram do usuário cadastrado no sistema BRVOZ pelo ID 34221, registrado em nome de Anderson José da Silva (CPF 089.144.179-48).

Foi igualmente verificado que partiram do mesmo usuário BRVOZ ID 34221 as ligações destinadas a outras autoridades públicas que também tiveram o aplicativo Telegram invadido de forma ilícita, tais como o Desembargador Abel Gomes (TRF 2ª região), o Juiz Federal Flávio Lucas (18ª Vara Federal do RJ) e os Delegados de Polícia Federal Rafael Fernandes (SR/PF/SP) e Flávio Vieitez Reis (DPF/CAS/SP).

Por sua vez, outras informações fornecidas pela BRVOZ demonstraram que o cliente BRVOZ ID 34221 possuía correlação com o cliente BRVOZ ID 69616. Nas declarações prestadas por Danilo Borges de Brito (Anexo 03 da medida cautelar nº 1017553-96.2019.4.01.3400), proprietário da BRVOZ, foi afirmado que após ter bloqueado a conta ID 34221, tendo em vista reclamações recebidas da empresa DATORA sobre a existência das chamadas suspeitas, ele recebeu uma ligação originada da conta ID 69916, cadastrada em nome de Marcelo Alexandre Thomaz (CPF 153.588.678-13). Nesta ligação, o interlocutor do ID 69616 se identifica como Anderson (nome registrado para o usuário BRVOZ ID 34221) e reclama do bloqueio de sua conta ID 34221.

Do mesmo modo, ao analisar os logs do sistema da BRVOZ, que realiza a gravação dos registros de IP das ligações, dentre outros dados, verificou-se que os ID 34221 e ID 16737, este último cadastrado em nome de Manoel C. Tenório (CPF 088.459.644-34), utilizaram o mesmo IP 189.33.65.37 várias vezes, em dias diferentes ou mesmo





MJSP - POLÍCIA FEDERAL
DIRETORIA DE INTELIGÊNCIA POLICIAL
COORDENAÇÃO-GERAL DE INTELIGÊNCIA
Divisão de Contraineligência Policial

concomitantemente. Por outro lado, analisando os *logs* das ligações foi possível identificar que os clientes BRVOZ ID 34221 e ID 16737 possuíam vários registros de ligações originadas e recebidas do número.

Conforme o Laudo de Perícia de Informática Laudo nº 1195/2019-INC/DITEC/PF, foi verificado que os clientes BRVOZ ID 34221, ID 16737 e ID 69916 realizaram 6.508 ligações em que o número de origem era igual ao número de destino, chamadas estas relacionadas a 1.330 números diferentes. Ainda estão sendo realizadas diligências visando a identificação de todas as vítimas dos ataques.

Por tais evidências, concluiu-se que os clientes BRVOZ ID 34221, ID 69916 e ID 16737 teriam algum tipo de relacionamento, tendo partido da conta ID 34221 todas as ligações de VoIP que permitiram o acesso às contas do aplicativo Telegram vinculadas a telefones utilizados pelo Ministro Sérgio Moro, pelo Desembargador Abel Gomes (TRF 2ª região), pelo Juiz Federal Flávio Lucas (18ª Vara Federal do RJ) e pelos Delegados de Polícia Federal Rafael Fernandes (SR/PF/SP) e Flávio Vieitez Reis (DPF/CAS/SP).

Conforme mencionado anteriormente, os cadastros dos usuários da BRVOZ identificados nos sistemas internos da empresa de telefonia, tais como os IDs 34221, 69916 e 16737, foram realizados com base em dados lançados pelos clientes no momento do preenchimento do sistema de emissão de boletos pela empresa PagSeguro, bem como em informações fornecidas à microempresa de telefonia em mensagens por e-mail.

Entretanto, verificou-se que não seriam verdadeiras as informações constantes nos sistemas da BRVOZ em relação ao cadastro das contas ID 34221, registrado em nome de Anderson José da Silva (CPF 089.144.179-48), ID 69616, cadastrada como sendo de Marcelo Alexandre Thomaz (CPF 153.588.678-13) e ID 16737, em nome de Manoel C. Tenório (CPF 088.459.644-34). Somente os dados relativos aos e-mails vinculados às referidas contas teriam alguma utilidade para as investigações, pois este seria o canal principal de comunicação entre a BRVOZ e os seus clientes.





MJSP - POLÍCIA FEDERAL
DIRETORIA DE INTELIGÊNCIA POLICIAL
COORDENAÇÃO-GERAL DE INTELIGÊNCIA
Divisão de Contraineligência Policial

Deste modo, para a identificação dos verdadeiros clientes BRVOZ ID 34221, ID 69916 e ID 16737 foi necessário verificar os endereços de protocolo da internet (endereço IP) atribuídos aos dispositivos (computador ou *smartphone*) que se conectaram ao serviço de telefonia VoIP da empresa BRVOZ no momento dos ataques.

Foram informados pelas provedoras os seguintes endereços IP como sendo aqueles utilizados pelos usuários BRVOZ ID 34221, ID 69916 e ID 16737 para realizar diversas ligações com o número de origem igual ao número discado:

- a) Endereço IP e porta 189.5.225.166:7966,5852,6297: cadastro em nome de DANILO CRISTIANO MARQUES, CPF370.074.428-54, localizado no endereço da Av. Leão XIII, 1700, apto. 162, Ribeirania, Ribeirão Preto/SP, e-mail ladanado@icloud.com;
- b) Endereço IP e porta 189.33.65.37:7190,8532,8317,8130 e 201.6.142.37:38021: cadastro em nome de MARTA MARIA ELIAS, CPF 034.843.538-05, endereço Rua Enga Amália Perola Casab, 415, BL 2, apt. 306, Parque Munhoz, São Paulo/SP, e-mail fernandotpsilva@hotmail.com;
- c) Endereço IP 179.182.157.130 e 191.250.245.225: cadastro em nome de SUELEN PRISCILA DE OLIVEIRA, CPF 427.742.138-51, localizado no endereço da Rua Maria do Carmo F Granato, nº 155, Jardim Roberto Selmi Dei, Araraquara/SP.

Em seguida, com base nos dados fornecidos pelos provedores de internet, foram realizadas diligências de campo visando a identificação dos moradores dos endereços onde estariam localizados os IPs de onde partiram os ataques. Assim, segundo a Informação nº 023/19 – DICINT/CGI/DIP/PF, foi identificado que no endereço da Av. Leão XIII, 1700, apto. 162, Ribeirania, Ribeirão Preto/SP, residia **WALTER DELGATTI NETO** (CPF 378.676.428-03),





MJSP - POLÍCIA FEDERAL
DIRETORIA DE INTELIGÊNCIA POLICIAL
COORDENAÇÃO-GERAL DE INTELIGÊNCIA
Divisão de Contrainteligência Policial

pessoa natural de Araraquara/SP, mesma cidade de nascimento de **DANILO CRISTIANO MARQUES** (CPF370.074.428-54), em nome de quem estava cadastrado o IP utilizado pelo usuário da BRVOZ ID 34221 para a realização das invasões dos dispositivos telefônicos das vítimas.

Por sua vez, segundo a Informação nº 023/19 – DICINT/CGI/DIP/PF, no endereço da Rua Enga Amália Perola Casab, 415, BL 2, apt. 306, Parque Munhoz, São Paulo/SP, residia **GUSTAVO HENRIQUE ELIAS SANTOS** (CPF 389.864.308-51), filho de MARTA MARIA ELIAS, pessoa em nome de quem estava cadastrado o IP também utilizado pelos clientes BRVOZ ID 34221 e ID 69916.

Ainda conforme a Informação nº 023/19 – DICINT/CGI/DIP/PF, foi constatado que **SUELEN PRISCILA DE OLIVEIRA**, também natural de Araraquara/SP, era namorada de GUSTAVO HENRIQUE ELIAS SANTOS e residia com ele naquele endereço da cidade de São Paulo/SP. Entretanto, o IP localizado na Rua Maria do Carmo F Granato, nº 155, Jardim Roberto Selmi Dei, Araraquara/SP também estava registrado em nome de SUELEN PRISCILA, conforme Informação nº 24/2019-DICINT (Anexo 07 da medida cautelar nº 1017553-96.2019.4.01.3400), tendo sido tal endereço selecionado também como de interesse para as investigações.

6 – DEFLAGRAÇÃO DA OPERAÇÃO SPOOFING

Em cumprimento à ordem judicial expedida no âmbito da medida cautelar em referência, no dia 23/07/2019 foi deflagrada a denominada Operação Spoofing, com a realização do cumprimento dos mandados de prisão temporária de WALTER DELGATTI NETO, DANILO CRISTIANO MARQUES, GUSTAVO HENRIQUE ELIAS SANTOS e SUELEN PRISCILA DE OLIVEIRA, além de ações de busca e apreensão nos seguintes locais de interesse para as investigações:





MJSP - POLÍCIA FEDERAL
DIRETORIA DE INTELIGÊNCIA POLICIAL
COORDENAÇÃO-GERAL DE INTELIGÊNCIA
Divisão de Contraineligência Policial

- a) EQUIPE 01: AV. LEÃO XIII, Nº 1700, APT. 162, RIBEIRANIA, CEP 14096-190 - RIBEIRÃO PRETO/SP (endereço de instalação de protocolo IP de onde partiram os ataques);
- b) EQUIPE 02: RUA ENGA AMÁLIA PEROLA CASAB, Nº 415, BL 2, APT. 306, PARQUE MUNHOZ, CEP 05782 - SÃO PAULO/SP (endereço de instalação de protocolo IP de onde partiram os ataques);
- c) EQUIPE 03: AVENIDA CATHARINA SUCCINI BOCCUCI, Nº 211 - CASA - JARDIM DAS PAINEIRAS, CEP 14807-280 - ARARAQUARA/SP (endereço vinculado a DANILO CRISTIANO MARQUES);
- d) EQUIPE 04: AVENIDA SANTA INES, Nº 838, VILA SANTA MARIA (VILA XAVIER), CEP 14810-033 - ARARAQUARA/SP (endereço vinculado a WALTER DELGATTI NETO);
- e) EQUIPE 05: RUA PROF MANOEL CERQUEIRA LEITE, Nº 642, JARDIM IMPERADOR, CEP 14806-267 - ARARAQUARA/SP (endereço vinculado a GUSTAVO HENRIQUE ELIAS SANTOS);
- f) EQUIPE 06: RUA MARIA DO CARMO F GRANATO, Nº 155, JARDIM ROBERTO SELMI DEI, ARARAQUARA/SP (endereço de instalação de protocolo IP de onde partiram os ataques);

Os dados e informações obtidas na ação de busca e apreensão no endereço vinculado a WALTER DELAGATTI NETO confirmaram que a Polícia Federal, ao executar a Operação Spoofing, havia de fato localizado os dispositivos utilizados nas invasões de contas do Telegram de diversas autoridades. As capturas de tela (*prints*) enviados à Polícia Federal indicavam que as seções do aplicativo não reconhecidas pelas vítimas estariam presentes, de forma geral, em um "iPhone XS Max, IOS 12.3.1" e em um "PC, Windows 10", modelos e sistemas compatíveis aos aparelhos apreendidos com o investigado. Também foi verificado de

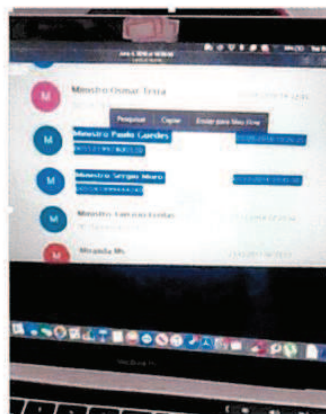




MJSP - POLÍCIA FEDERAL
DIRETORIA DE INTELIGÊNCIA POLICIAL
COORDENAÇÃO-GERAL DE INTELIGÊNCIA
Divisão de Contrainteligência Policial

imediatos que tais dispositivos estavam configurados para acesso a múltiplos perfis do aplicativo Telegram de terceiros, sendo o iPhone XS Max por meio dos aplicativos Telegram e Telegram X e o notebook Lenovo por meio do aplicativo Telegram Desktop.

Também sobre a mesa ao lado da cama foi encontrado, desligado, um computador portátil da marca Apple, modelo Macbook Pro A1706, número de série C02WL1FUHV2N, arrecadado como item 1 do Auto Circunstanciado de Busca e Apreensão. Uma vez introduzida a senha, foi possível visualizar a área de trabalho do usuário "Red Redinho". Segundo os Peritos Criminais da Polícia Federal, uma das janelas de aplicativo abertas exibiu uma imagem datada de 4 de junho de 2019, cuja análise inicial indicou tratar-se de fotografia ou captura de tela de dispositivo que exibiu lista de contatos de determinado perfil não identificado do Telegram, dentre os quais Ministro Osmar Terra, Ministro Paulo Guedes, Ministro Sérgio Moro e Ministro Tarcísio Freitas (figura abaixo):



O investigado espontaneamente orientou os Peritos Criminais Federais a localizar as pastas com arquivos de dados de diversas pessoas, que teriam sido obtidos por meio de acesso indevido a contas do aplicativo Telegram. Os Peritos não acessaram o conteúdo dos referidos arquivos, no entanto foi possível constatar, ao menos no caso do perfil vinculado ao número +55(41)984014762, que o tipo e a estrutura das pastas de arquivos eram compatíveis

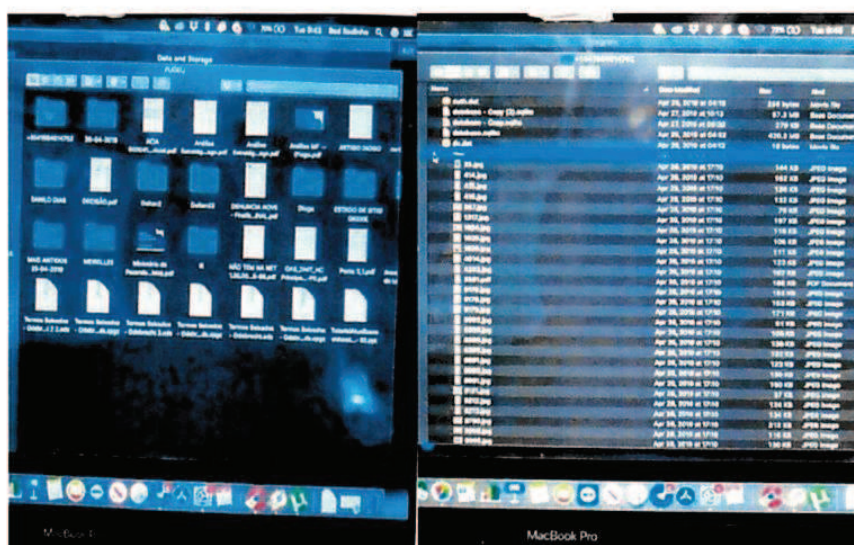
[Assinatura manuscrita]





MJSP - POLÍCIA FEDERAL
DIRETORIA DE INTELIGÊNCIA POLICIAL
COORDENAÇÃO-GERAL DE INTELIGÊNCIA
Divisão de Contrainteligência Policial

com uma extração realizada a partir dos servidores do aplicativo Telegram, por meio de ferramenta similar ao programa por linha de comandos "Telegram_Backup", conforme figuras abaixo:



Foram ainda reunidas outras evidências da participação direta de WALTER DELGATTI NETO nas invasões de dispositivos informáticos de inúmeras autoridades públicas do país. Em suas declarações à Polícia Federal (fls 80/83), WALTER DELGATTI NETO confirmou ter obtido o código de acesso do Telegram e criado uma conta no referido aplicativo vinculada ao número telefônico do Ministro da Justiça e Segurança Pública Sérgio Moro, além de admitir ser também o responsável pela invasão de contas do aplicativo de diversas outras autoridades públicas.

Do mesmo modo, WALTER DELGATTI NETO confirmou que repassou ao jornalista Glenn Greenwald, editor do The Intercept Brasil o conteúdo de mensagens do Telegram referentes a conversas realizadas entre os Procuradores da República que atuam na força-tarefa da operação Lava Jato, no estado do Paraná, tendo ressaltado que nunca recebeu





**MJSP - POLÍCIA FEDERAL
DIRETORIA DE INTELIGÊNCIA POLICIAL
COORDENAÇÃO-GERAL DE INTELIGÊNCIA
Divisão de Contraineligência Policial**

qualquer valor, quantia ou vantagem em troca do material que disponibilizou. Também foi relatado por WALTER DELGATTI NETO que não conheceu pessoalmente Glenn Greenwald ou qualquer outro jornalista da equipe do The Intercept e que em nenhum momento teria repassado seus dados pessoais.

Também foram encontrados indicativos do envolvimento de WALTER DELGATTI NETO, DANILO CRISTIANO MARQUES, GUSTAVO HENRIQUE ELIAS SANTOS e SUELEN PRISCILA DE OLIVIERIA no cometimento sistemático de fraudes bancárias e estelionatos eletrônicos, inclusive com a apreensão de valores em espécie e diversos cartões bancários em nome de terceiros, além da localização de inúmeros arquivos e programas utilizados na obtenção de senhas e dados de suas vítimas, bem como ações voltadas à ocultação ou dissimulação da origem dos recursos de origem ilícita, configurando em tese o delito de lavagem de dinheiro, conforme disposto no artigo 1º da Lei nº 9.613/98.

Assim, para a conveniência da instrução criminal e para assegurar a aplicação da lei penal, foi determinada a prisão preventiva de WALTER DELGATTI NETO, DANILO CRISTIANO MARQUES, GUSTAVO HENRIQUE ELIAS SANTOS e SUELEN PRISCILA DE OLIVEIRA.

Entretanto, mesmo com a apreensão dos equipamentos utilizados no ataque a contas do Telegram de autoridades públicas, ainda caberia às investigações o preenchimento de algumas lacunas informacionais, como a identificação de outros envolvidos nas invasões, o período em que os crimes foram cometidos ou a existência de possíveis mandantes, coautores ou mentores intelectuais dos crimes, com a delimitação de suas condutas de forma individualizada.

7 – SEGUNDA FASE DA OPERAÇÃO SPOOFING

Em suas declarações iniciais, WALTER DELGATTI NETO alegou ter sido o único responsável pelo desenvolvimento e aplicação da técnica utilizada para invadir contas do





MJSP - POLÍCIA FEDERAL
DIRETORIA DE INTELIGÊNCIA POLICIAL
COORDENAÇÃO-GERAL DE INTELIGÊNCIA
Divisão de Contrainteligência Policial

Telegram de autoridades públicas. Entretanto, após a análise dos arquivos armazenados nos dispositivos telemáticos apreendidos com WALTER NETO, foi possível perceber o envolvimento de ao menos outras duas pessoas nos fatos investigados:

- i) LUIZ HENRIQUE MOLIÇÃO, que teria atuado diretamente na invasão, na interceptação e divulgação de comunicações realizadas pelas vítimas através do aplicativo *Telegram*; e
- ii) THIAGO ELIZER MARTINS SANTOS, que atuaria no desenvolvimento de técnicas voltadas à invasão de redes de computadores e comunicação e teria conhecimento e participação nos crimes cibernéticos cometidos por WALTER DELGATTI NETO.

A participação de LUIZ HENRIQUE MOLIÇÃO nos fatos foi percebida após a análise do arquivo "áudio_2019-06-07_20-22-05.ogg", datado de 07/06/2019, três dias após o ataque ao celular do Senhor Ministro Sérgio Moro, que foi encontrado no *Macbook Pro* de WALTER NETO (item 01 da Equipe 01 – Operação *Spoofing*) conforme Informação nº 32/2019-DICINT/CGI/DIP (anexo 01 da medida cautelar nº 1015706-59.2019.4.01.3400),

Referido arquivo contém uma gravação em áudio da conversa realizada entre um homem até então não identificado (HNI) e o jornalista GLENN EDWARD GREENWALD, do portal de notícias *The Intercept*, autor de várias reportagens elaboradas com base em material obtido através da invasão de contas do aplicativo *Telegram*. Na referida gravação, o HNI, aparentemente bastante jovem, trava um diálogo com Glenn Greenwald, e menciona que "a gente" ou o "grupo" pegou o *Telegram* de várias pessoas no ano passado (2018):

GLENN GREENWALD: *Tudo bom?*

HNI: *Então é... a gente...eu estava discutindo com o grupo... eu queria falar com você um assunto.*

GLENN: *Hã...*

HNI: *É... como tá agora tá saindo muita notícia sobre isso, a gente chego... nós..*





MJSP - POLÍCIA FEDERAL
DIRETORIA DE INTELIGÊNCIA POLICIAL
COORDENAÇÃO-GERAL DE INTELIGÊNCIA
Divisão de Contraineligência Policial

GLENN: Sim

HNI: ...chegamos à conclusão que eles estão fazendo um jogo pra tentar desmoralizar o que tá acontecendo.

GLENN: Há ham

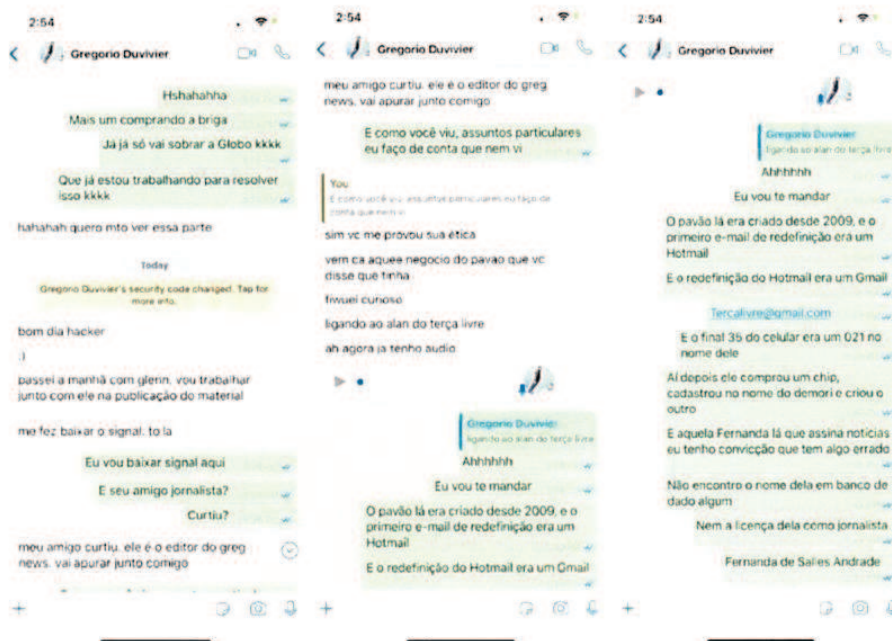
HNI: Igual o que aconteceu com o Danilo Gentile, é... o MBL, o Holiday... a gente pegou outubro do ano passado. Eles estão começando a falar isso agora. ... (segue)

Por sua vez, conforme Informação nº 33/2019-DICINT/CGI/DIP/PF (anexo 02 da medida cautelar nº 1027025-24.2019.4.01.3400), durante as análises do celular apreendido com WALTER DELGATTI foram encontradas mensagens do aplicativo *WhatsApp* trocadas com a pessoa identificada como "MOLIÇÃO", vinculado ao celular de nº +55(16)99111-8526. Nessas mensagens, datadas de 15/07/2019, WALTER NETO envia para MOLIÇÃO fotos de tela (*prints*) de uma conversa que teria ele realizado com Gregório Duvivier, conhecido ator e escritor, sobre a publicação do material repassado para Glenn Greenwald, além de tratarem sobre um assunto que envolveria a pessoa denominada "PAVÃO":





MJSP - POLÍCIA FEDERAL
DIRETORIA DE INTELIGÊNCIA POLICIAL
COORDENAÇÃO-GERAL DE INTELIGÊNCIA
Divisão de Contrainteligência Policial

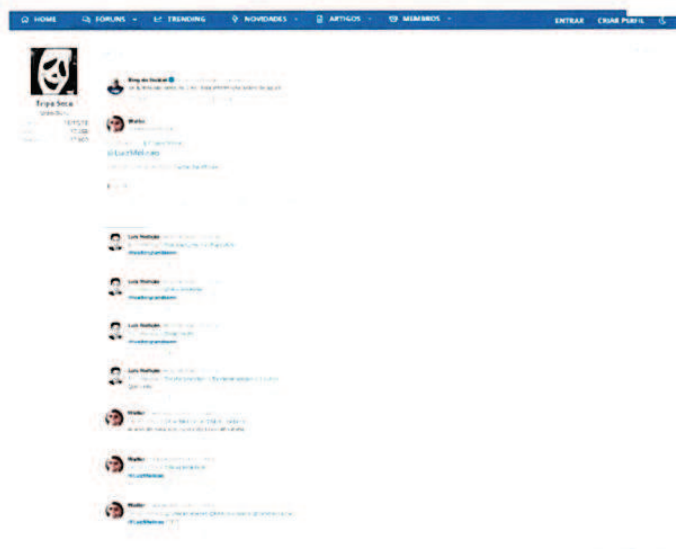


Com base na análise dessas mensagens, foram realizadas pesquisas que permitiram a identificação do interlocutor de WALTER NETO como sendo LUIZ HENRIQUE MOLIÇÃO (CPF 498.486.768-05), que possuiria no *Twitter* o perfil “@LuizMolicao” e no *Instagram* a conta “@luiz.molicao”. Pesquisas em fontes abertas também identificaram o site <https://forum.politz.com.br/threads/bondedaoposicao-orcrim-se-blinda-camara-aprovalei-anti-lava-jato-lei-de-abuso-de-autoridade-lider-do-pcc-diz-ter-mantido-dialogo-com-opt.266/page-6586>, onde o nome e o perfil do *Twitter* de LUIZ MOLIÇÃO eram citados, juntamente com o perfil do *Twitter* de WALTER DELGATTI, com referência ao episódio da “clonagem” da conta do *Telegram* do Ministro Paulo Guedes:





MJSP - POLÍCIA FEDERAL
DIRETORIA DE INTELIGÊNCIA POLICIAL
COORDENAÇÃO-GERAL DE INTELIGÊNCIA
Divisão de Contrainteligência Policial



Analisando o perfil de Instagram “@luiz.molicao” foi identificado um vídeo no *stories* no qual foi possível ouvir a voz de LUIZ MOLICÃO, que segundo a equipe policial, aparentava ter semelhança com a voz do interlocutor do jornalista Glenn Greenwald na gravação de áudio acima mencionada (Informação nº 33/2019-DICINT/CGI/DIP/PF - anexo 02 da medida cautelar nº 1027025-24.2019.4.01.3400). Por tais informações, verificou-se a existência de indícios razoáveis da participação de LUIZ HENRIQUE MOLICÃO nos fatos investigados.

Já o nome de THIAGO ELIEZER MARTINS SANTOS surgiu nas investigações como um dos suspeitos de participar do grupo de fraudadores cibernéticos (*hackers*) investigado, tendo em vista as diversas evidências que foram reunidas na Informação nº 32/2019-DICINT//DIP/PF (anexo 01 medida cautelar nº 1027025-24.2019.4.01.3400). A equipe de análise policial verificou que o telefone celular nº (61)99103-1432, que segundo bases de dados da Polícia Federal pertence a THIAGO ELIEZER MARTINS SANTOS, aparece como destinatário de várias ligações realizadas pelo cliente da BRVOZ ID 34221, número de usuário

10





MJSP - POLÍCIA FEDERAL
DIRETORIA DE INTELIGÊNCIA POLICIAL
COORDENAÇÃO-GERAL DE INTELIGÊNCIA
Divisão de Contrainteligência Policial

vinculado a WALTER DELGATTI NETO na empresa de telefonia de voz sobre IP (VoIP) denominada BRVOZ (MEGAVOIP).

Ressalte-se novamente, que partiram do ID 34221 as ligações em voz sobre IP (VoIP), realizadas por WALTER DELGATTI NETO através do sistema da BRVOZ com a alteração do número chamador, que permitiram o acesso à caixa postal dos telefones das vítimas e a consequente obtenção dos códigos das contas do Telegram que foram invadidas. Por sua vez, verificou-se que WALTER DELGATTI NETO realizou ligações para o número (61)99103-1432 sem manipular o número chamador no sistema da BRVOZ, ou seja, o cliente BRVOZ ID 34221, que realizou a maioria dos ataques a dispositivos informáticos de autoridades públicas, também teria efetuado diversas chamadas para THIAGO ELIEZER MARTINS SANTOS, porém sem mascarar o número verdadeiro que originou as chamadas.

Ainda segundo a Informação nº 32/2019-DICINTI/DIP/PF (anexo 01 da medida cautelar nº 1015706-59.2019.4.01.3400), o telefone de THIAGO ELIEZER MARTINS SANTOS (61- 99103-1432) aparece em vários registros de ligações originadas e/ou recebidas pela conta ID 42680, que é cadastrada na empresa BRVOZ em nome de João Rodrigues Filho (CPF 103.715.245-04), com endereço residencial em Brasília-DF. Porém, diversos bancos de dados apontam que João Rodrigues residiria no Estado de Sergipe, fato que indicava que o cadastro na BRVOZ do usuário ID 42680 havia sido realizado com nome falso, assim como ocorreu em relação às contas na BRVOZ que também eram utilizadas por WALTER DELGATTI NETO e GUSTAVO HENRIQUE ELIAS SANTOS para realizar ligações VoIP com a edição do número chamador.

Verificou-se, do mesmo modo, que os registros de ligações da conta BRVOZ ID 42680 possui histórico muito semelhante daquelas contas na empresa de telefonia de VoIP que eram utilizadas por WALTER DELGATTI NETO e GUSTAVO HENRIQUE ELIAS, quando a grande maioria dos números de origem eram manipulados e substituídos por números de instituições bancárias. Esses registros de chamadas indicavam, assim, que o cliente BRVOZ





MJSP - POLÍCIA FEDERAL
DIRETORIA DE INTELIGÊNCIA POLICIAL
COORDENAÇÃO-GERAL DE INTELIGÊNCIA
Divisão de Contrainteligência Policial

ID 42680 também estaria envolvido com fraudes bancárias eletrônicas e outros crimes cibernéticos.

De acordo com a informação nº 32/2019-DICINT//DIP/PF (anexo 01 da medida cautelar nº 1015706-59.2019.4.01.3400), foi informado pelo provedor de acesso à internet que o usuário BRVOZ ID 42680 acessou no dia 23/05/2019 a mesma rede IP (protocolo de endereço da internet) que era utilizada por WALTER DELGATTI NETO (2804:14D:5883:A0AF:D832:F4D6:A133:7292", instalado na Av. Leão XIII, 1700, apto 162 Ribeirinha, Ribeirão Preto/SP). Por sua vez, conforme informação enviada pela empresa provedora de internet (anexo 12), outros IPs utilizados pelo usuário BRVOZ ID 42680 (IP 189.6.22.182 - Porta 27530) estavam registrados no endereço da QNB, Qd 13, casa 22, Taguatinga Brasília/DF - CEP 72.115-130, em nome de DENISE MARIA MARTINS SANTOS, que é mãe de THIAGO ELIEZER MARTINS SANTOS.

Em sua primeira oitiva à Polícia Federal, WALTER DELGATTI NETO foi questionado sobre quem seria THIAGO ELIEZER MARTINS SANTOS, tendo se reservado ao direito de permanecer em silêncio (anexo 02 da medida cautelar nº 1015706-59.2019.4.01.3400). Por sua vez, na segunda declaração que prestou a este órgão policial (30/07/2019), WALTER NETO confirmou que de fato conheceu pela internet THIAGO ELIEZER MARTINS SANTOS, de quem teria comprado um veículo Land Rover por volta de dezembro de 2018 (anexo 03 da medida cautelar nº 1015706-59.2019.4.01.3400). WALTER NETO alegou que somente se encontrou pessoalmente com THIAGO ELIEZER quando veio a Brasília/DF buscar o veículo que teria adquirido, tendo THIAGO ELIEZER o levado do aeroporto para o hotel em Brasília/DF. Entretanto, WALTER NETO não soube dizer qual seria o nome ou o endereço do hotel em que teria ficado hospedado, detalhe que impediu a confirmação dessa versão dos fatos pela Polícia Federal.

Em razão da execução da fase ostensiva da Operação Spoofing, seria natural que envolvidos ainda não alcançados pelas investigações adotassem contramedidas visando a ocultação e/ou a eliminação de evidências, do mesmo modo que, pelas características

36





MJSP - POLÍCIA FEDERAL
DIRETORIA DE INTELIGÊNCIA POLICIAL
COORDENAÇÃO-GERAL DE INTELIGÊNCIA
Divisão de Contrainteligência Policial

de atuação do grupo, novos suspeitos provavelmente iriam se evadir caso fossem simplesmente intimados a comparecer à Polícia Federal, em data e local previamente agendados. Assim, foi considerada a adoção de medida cautelar de interceptação de comunicações telefônicas e telemáticas visando aumentar o grau de eficácia das diligências investigativas em relação ao envolvimento de THIAGO ELIEZER MARTINS SANTOS e LUIZ HENRIQUE MOLIÇÃO nos fatos sob apuração.

As circunstâncias concretas do presente caso exigiam um esforço concentrado para a conclusão das apurações com celeridade e eficiência, tendo a interceptação das comunicações telefônicas de THIAGO ELIEZER se mostrado uma medida bastante útil para as investigações, na medida em que possibilitou a identificação da residência de sua namorada, ANA BEATRIZ MACHADO D'ALMEIDA, como local de interesse para as investigações, tendo em vista os fortes indícios de que o investigado utilizava o local para ocultar da Polícia Federal provas ou evidências de suas participação nos crimes.

Assim, em cumprimento à ordem judicial expedida no âmbito da medida cautelar nº 1027025-24.2019.4.01.3400, foi deflagrada a Operação Spoofing II, com o cumprimento dos mandados de prisão temporária de LUIZ HENRIQUE MOLIÇÃO e THIAGO ELIEZER MARTINS, bem como a realização de ações de busca e apreensão nos seguintes locais de interesse para as investigações:

- a) EQUIPE 01: QNB13, CASA 22, TAGUATINGA NORTE – BRASÍLIA/DF (endereço de Denise Maria Martins Santos (mãe), local onde THIAGO ELIEZER estaria residindo atualmente, conforme informações do NO/DICINT. Ressalta-se também, que o IP que acessou a conta da BRVOZ ID 42680 estaria instalado neste endereço).
- b) EQUIPE 03: RUA SANTO AMARO, 341, EDIFÍCIO FORTUNA, APARTAMENTO 1605 ou 1065, BELA VISTA, SÃO PAULO/SP (endereço residencial, de ANA BEATRIZ MACHADO, namorada de





MJSP - POLÍCIA FEDERAL
DIRETORIA DE INTELIGÊNCIA POLICIAL
COORDENAÇÃO-GERAL DE INTELIGÊNCIA
Divisão de Contrainteligência Policial

THIAGO ELIEZER MARTINS SANTOS. Foi verificado que THIAGO ELIEZER viaja constantemente para a cidade de São Paulo/SP e, nas oportunidades verificadas, ele se hospeda neste endereço);

- c) RUA GIACOMO MERITANO CORTEZE, 481, SERTAOZINHO – SP:
(endereço residencial de LUIZ HENRIQUE MOLIÇÃO)

Após a oitiva dos investigados e análise do material arrecadado, foram reunidos diversos elementos de prova que reforçaram o envolvimento de LUIZ HENRIQUE MOLIÇÃO nas invasões de dispositivos informáticos de autoridades públicas brasileiras. Por sua vez, THIAGO ELIEZER MARTINS SANTOS confirmou que tinha conhecimento da técnica utilizada por WALTER DELGATTI NETO para invadir contas do Telegram de outras pessoas, sendo também usuário dos mesmos *softwares* e serviços de voz sobre IP (VOIP) da empresa BRVOZ (MEGAVOIP) que foram utilizados na interceptação de comunicações de autoridades públicas.

Também foram encontradas durante as investigações evidências do envolvimento de THIAGO ELIEZER no cometimento sistemático de crimes cibernéticos, além de fraudes bancárias por meio de ataques realizados via internet, quando são utilizados diversos métodos visando a obtenção de senhas e dados de suas vítimas. Assim, para a conveniência da instrução criminal e para assegurar a aplicação da lei penal, foi igualmente determinada a prisão preventiva de LUIZ HENRIQUE MOLIÇÃO e THIAGO ELIEZER MARTINS SANTOS.

8 – ELEMENTOS DE PROVA COLETADOS NAS DUAS FASES DA OPERAÇÃO SPOOFING

Com a deflagração das duas fases da Operação Spoofing, fora coletado vasto material de interesse para as investigações, com destaque para os diversos dispositivos eletrônicos contendo dados armazenados. Ao todo, foram reunidos cerca de **7 TB** de dados eletrônicos, que se encontravam em dispositivos diversos, tais como *smartphones*, *notebooks*, *hard disks* (HD), *pen drives*, *tablets* e outros dispositivos de mídia de armazenamento de dados.





MJSP - POLÍCIA FEDERAL
DIRETORIA DE INTELIGÊNCIA POLICIAL
COORDENAÇÃO-GERAL DE INTELIGÊNCIA
Divisão de Contraineligência Policial

Todos os dispositivos arrecadados foram submetidos a exames pelo Serviço de Perícias em Informática do Instituto Nacional de Criminalística da Polícia Federal, que objetivaram a extração e análise do conteúdo do material, com a elaboração de Laudo Pericial de Informática específico para cada item apreendido. Os arquivos das mídias passaram por um processo de garantia de integridade baseado no algoritmo *Secure Hash Algorithm* (SHA) de 256 bits, cujos resultados foram registrados em arquivos denominados "hashes.txt" e anexados em mídia ótica a cada um dos Laudos. Dessa forma, qualquer alteração do conteúdo em anexo aos Laudos (remoção, acréscimo, alteração de arquivos ou parte de arquivos), bem como sua substituição por outro com teor diferente, pode ser detectada.

A extração de dados dos aparelhos e dispositivos de armazenamento eletrônico foi realizada exclusivamente de forma automatizada, por meio de ferramenta forense apropriada. Para a extração dos dados dos aparelhos celulares, *notebook* e *tablets* foi utilizado o equipamento Cellebrite UFED 4PC, bem como o *software* Cellebrite Physical Analyzer para a geração de relatórios. Por sua vez, os relatórios gerados foram submetidos a processamento por meio do programa Indexador e Processador de Evidências Digitais – IPED, o qual realiza a categorização dos dados, permite buscas indexadas, a pré-visualização do conteúdo dos arquivos, bem como apresenta diversos atributos dos arquivos categorizados, tais como datas de criação e acesso, localização no sistema de arquivos, valor da função de resumo criptografado MD5 e se o arquivo encontra-se com o status de apagado ou não, dentre outras funcionalidades.

O conteúdo dos dispositivos de armazenamento computacional foi duplicado para arquivos de imagem forense, juntamente com a ferramenta gráfica para a análise de dados gerados pelo IPED (IPED-SearchApp.exe), sendo então copiado para mídias encaminhadas em anexo aos laudos. Por motivo segurança, foram enviadas à equipe policial de investigação e análise somente as cópias dos materiais, preservando-se os originais. Com a finalidade de materializar as informações obtidas durante as análises dos dados armazenados nos dispositivos, e após serem confrontados e complementados com outros dados que guardam





MJSP - POLÍCIA FEDERAL
DIRETORIA DE INTELIGÊNCIA POLICIAL
COORDENAÇÃO-GERAL DE INTELIGÊNCIA
Divisão de Contraineligência Policial

relação com os fatos em investigação, foram elaborados dois tipos de documentos específicos: i) Informações de exploração de material apreendido, contendo fato relevante de interesse investigativo, que tem como finalidade formalizar a atribuição de sentido aos dados apreendidos e sua vinculação com a hipótese criminal; e ii) o Relatório de Análise de Material Apreendido, referente ao resumo das evidências encontradas em um determinado item apreendido na ação de busca e apreensão.

Segue abaixo tabela com informações referentes aos itens de armazenamento de dados apreendidos, o Laudo Pericial a que está vinculado, descrição do dispositivo periciado e o Relatório de Análise de Material Apreendido (RAMA) respectivo, caso tenha sido elaborado:

ALVO	Eq.	Item	Laudo	Descrição	RELATÓRIO DE ANÁLISE DE MATERIAL - RAMA
Walter Delgatti Neto	1	1	1409/2019 e 1458/2019	Nootebook marca Apple, modelo MACBOOK Pro A1706 EMC3163, serial C02WL1FUHV2N, FCC ID: BCGA1706, IC: 579C-A1706, com uma fonte de alimentação	04/2019 DICINT/CGI/DIP/PF
Walter Delgatti Neto	1	2	1409/2019 e 1458/2019	Um notebook marca LENOVO, cor preto, modelo I520-15IKBN 80 WK, série n° PF0RV8MR - MTM 80WK003QCL, ID: JVHFC1, com uma fonte de alimentação	29/2019 DICINT/CGI/DIP/PF
Walter Delgatti Neto	1	3	1409/2019 e 1458/2019	Um PenDrive preto com proteção metálica semelhante a cor cinza prata, com capacidade de 8G	15/2019 DICINT/CGI/DIP/PF
Walter Delgatti Neto	1	4	1409/2019 e 1458/2019	Um mini Compact Disc Recordable High Speed de capacidade de 25 minutos e 225 MegaBytes	NÃO SE APLICA
Walter Delgatti Neto	1	16	1409/2019 e 1458/2019	Um HD externo marca SEAGATE, série n° NAA87W8D, P/N° 1TEAPS-500, com capacidade de armazenamento de 1 Terabyte	23/2019 DICINT/CGI/DIP/PF





MJSP - POLÍCIA FEDERAL
DIRETORIA DE INTELIGÊNCIA POLICIAL
COORDENAÇÃO-GERAL DE INTELIGÊNCIA
Divisão de Contraineligência Policial

Walter Delgatti Neto	1	17	1409/2019 e 1458/2019	Um case com HD externo marca CB TECH, case USB 2.0, modelo CH-200, série número WDE69EBW, mobile HDD, ostentando a capacidade de armazenamento de 1TB	24/2019 DICINT/CGI/DIP/PF
Walter Delgatti Neto	1	20	1409/2019	Um Chip da Operadora VIVO sem numeração, localizado no interior do veículo JIPE Discovery NQT 7141	NÃO SE APLICA
Walter Delgatti Neto	1	21	1409/2019	Um Pen Drive da marca ScanDisk, vermelho e preto, Cruzer Blade, ostentando a capacidade de 8GB com as inscrições SDCZ50-008 G D33724 B 11604255058, Made in China	15/2019 DICINT/CGI/DIP/PF
Walter Delgatti Neto	1	18	1488/2019 e 1690/2019 Inf Tec 161/2019	Um aparelho celular da marca Apple, modelo iPhone XS Max nº T552BZ1A, série nº F2LXHEA8KPH6, IMEI 357287092232596 e IMEI 57287092443441, o qual continha em seu interior o Chip da operadora CLARO 89550 53297 02009 81594 AAC 006 HLRQOA, sem carregador. Senha de acesso: 1804.	43/2019 DICINT/CGI/DIP/PF
Walter Delgatti Neto	1	5	1515/2019 e 1690/2019 Inf. Tec 161/2019	Um telefone celular da marca Apple, modelo iPhone A 1533, com identificação FCC ID: BCG E2642A, IC579C E2642B, IMEI 013 988 000262163, contendo instalado no interior um Chip da Operadora Vivo 4G, identificação 8955101943 900136375838, sem carregador. Senha de acesso: 9196	14/2019 DICINT/CGI/DIP/PF
Walter Delgatti Neto	1	6	1515/2019 e 1690/2019 Inf Tec 161/2019	Um celular da marca Samsung, modelo SM G9201, cor branca, identificação FCC ID: A3LSMG9201, SÉRIE Nº RQ8GB4028Z9Z, IMEI 59590/06/038556/1, sem carregador.	17/2019 DICINT/CGI/DIP/PF
Gustavo e Suelen	2	44	1410/2019 e 1459/2019	Um drone marca MAVIC, modelo M1P, série nº 08QCEC4022Q4U6, password: 317e2c38, com case e kit contendo carregador de baterias, 05 baterias e um controle remoto, acondicionado em uma mala prata metálica da VONDER	NÃO SE APLICA





MJSP - POLÍCIA FEDERAL
DIRETORIA DE INTELIGÊNCIA POLICIAL
COORDENAÇÃO-GERAL DE INTELIGÊNCIA
Divisão de Contraineligência Policial

Gustavo e Suelen	2	48	1410/2019 e 1459/2019	Um notebook da marca Apple, modelo MACBOOK A534, na cor prata dourado, Serial C02Q13HBGF84, com um carregador	CRIOGRAFADO
Gustavo e Suelen	2	49	1410/2019 e 1459/2019	Um notebook da marca DELL, modelo INSPIRION N5110, na cor black piano, Serial J571751, com um carregador	16/2019 DICINT/CGI/DIP/PF
Gustavo e Suelen	2	50	1410/2019 e 1459/2019	Um notebook da SAMSUNG, modelo NP800G6H, na cor preta, serial 08839QAK400167V, com um carregador	25/2019 DICINT/CGI/DIP/PF
Gustavo e Suelen	2	51	1410/2019 e 1459/2019	Um notebook da marca DELL, modelo P53G, na cor preto, Serial G99P442, com um carregador	44/2019 DICINT/CGI/DIP/PF
Gustavo e Suelen	2	34	1475/2019	Um Tablet azul, da marca Multilaser, modelo M7, - 3G Plus, contendo uma etiqueta adesiva com o numero manuscrito 773.491.568-04	18/2019 DICINT/CGI/DIP/PF
Gustavo e Suelen	2	36	1493/2019	Um tablet azul, da marca Multilaser, modelo M7-3G PLUS, constando uma etiqueta de papel com o manuscrito CPF 277.099.508-17	20/2019 DICINT/CGI/DIP/PF
Gustavo e Suelen	2	39	1497/2019 e 1704/2019 Inf Tec 161/2019	Um iPhone branco sem IMEI. Localizado no quarto com Gustavo Henrique Elias Santos	08/2019 DICINT/CGI/DIP/PF
Gustavo e Suelen	2	31	1510/2019 e 1704/2019 Inf Tec 161/2019	Um aparelho de telefone celular da marca Apple, modelo iPhone, ostentando o IMEI 3591 430 7065 1992.	09/2019 DICINT/CGI/DIP/PF
Gustavo e Suelen	2	33	1521/2019 e 1704/2019 Inf Tec 161/2019	Um aparelho telefonico celular da marca Apple, modelo iPhone	03/2019 DICINT/CGI/DIP/PF
Gustavo e Suelen	2	32	1523/2019 e 1704/2019 Inf Tec 161/2019	Um aparelho telefonico celular da marca Apple, modelo iPhone, cor preta, ostentando o IMEI 3520530685229976	22/2019 DICINT/CGI/DIP/PF





MJSP - POLÍCIA FEDERAL
DIRETORIA DE INTELIGÊNCIA POLICIAL
COORDENAÇÃO-GERAL DE INTELIGÊNCIA
Divisão de Contraineligência Policial

Gustavo e Suelen	2	38	1528/2019	Um tablet preto, da marca Multilaser, modelo M7-3G PLUS, constando a identificação em etiqueta com os IMEIS 3531740994440886 e 353174094440894	10/2019 DICINT/CGI/DIP/PF
Gustavo e Suelen	2	35	1509/2019	Um tablet dourado, da marca Multilaser, modelo M7-3G PLUS, constando duas identificações a primeira com os IMEIS 353280090569154 e 353280090599151 e a segunda etiqueta, de papel constando o telefone e (31) 99815-3024 e 006.904.496-15	19/2019 DICINT/CGI/DIP/PF
Gustavo e Suelen	2	37	1516/2019	Um tablet dourado, da marca Multilaser, modelo M7-3G PLUS, constando duas identificações a primeira com os IMEIS 353280090569741 e 353280090599748 e a segunda etiqueta, de papel constando o telefone (21) 97207-2808 e 105.842.137-94	21/2019 DICINT/CGI/DIP/PF
Danilo Cristiano Marques	3	1	1446/2019 e 1590/2019	Um SSD, S/N 50026B777300F556 KINGSTON - 240 GB (retirado do Desktop)	05/2019 DICINT/CGI/DIP/PF
Danilo Cristiano Marques	3	2	1446/2019 e 1590/2019	Um HD WESTERN DIGITAL 500GB, 16MB cache S/N WCAYUF848172 (retirado dos desktop)	06/2019 DICINT/CGI/DIP/PF
Danilo Cristiano Marques	3	3	1446/2019 e 1590/2019	Um SSD (retirado do notebook), S/N S1C6J56Q745945, MODEL HH160HI, marca SEMP TOSHIBA	07/2019 DICINT/CGI/DIP/PF
Danilo Cristiano Marques	3	7	1548/2019 (ou 1550 - verificar) Inf Tec 161/2019	Um celular IPHONE 8 (possivelmente) registrado na Anatel sob o nº 051481701993	12/2019 DICINT/CGI/DIP/PF
Gustavo Henrique	6	24	1402/2019	Relógio da marca aparente ROLEX	NÃO SE APLICA
Gustavo Henrique Elias Santos	6	1	1432/2019 e 1588/2019	Um Modem TP-Link, mode TL-Wa855RE, SN: 217556008038 BR/2.0	NÃO SE APLICA
Gustavo Henrique Elias Santos	6	3	1432/2019 e 1588/2019	Um Notebook Sony Vaio modelo SVF152C29X com fonte	45/2019 DICINT/CGI/DIP/PF





MJSP - POLÍCIA FEDERAL
DIRETORIA DE INTELIGÊNCIA POLICIAL
COORDENAÇÃO-GERAL DE INTELIGÊNCIA
Divisão de Contraineligência Policial

Gustavo Henrique Elias Santos	6	13	1432/2019 e 1588/2019	Um Modem MitraStar GPT-2541GNAC s/n S150y44002505 nome REPE WiFi Fibra-sF1C	NÃO SE APLICA
Gustavo Henrique Elias Santos	6	15	1432/2019 e 1588/2019	Sete Pen-drives	39/2019 DICINT/CGI/DIP/PF
Gustavo Henrique Elias Santos	6	16	1432/2019	Um CD-R Multilaser 700MB sem inscrição.	NÃO SE APLICA
Gustavo Henrique Elias Santos	6	33	1432/2019	Um Modem USB 3G + Wn31 IMEI 356360045208228	NÃO SE APLICA
Gustavo Henrique Elias Santos	6	34	1432/2019	Três Chips de memória das câmeras da casa com a identificação frente-lado direito, frente-lado esquerdo. garagem, fundo, sala.	NÃO SE APLICA
Gustavo Henrique Elias Santos	6	39	1432/2019	Um Roteador Wireless 150Mbps LinkOne 90671018442112572.	NÃO SE APLICA
Gustavo Henrique Elias Santos	6	40	1432/2019	Um Modem FiberHome com a inscrição 4211	NÃO SE APLICA
Gustavo Henrique Elias Santos	6	41	1432/2019	Um DVD-R 16X sem inscrição	NÃO SE APLICA
Gustavo Henrique Elias Santos	6	44	1432/2019	Um HD Seagate 250GB n 6VYD4kBV	NÃO SE APLICA
Gustavo Henrique Elias Santos	6	51	Inf Tec 157/2019	Um iPhone rosa modelo 8 plus (equivale ao Item 28 devido a um erro na numeração do auto circunstanciado de arrecadação)	NÃO SE APLICA
Wisllen Francisco Delgatti	4	1	1550/2019 e Inf Tec 161/2019	Aparelho celular iPhone XR cor azul com IMEI 357368094369055 com senha: 100390	40/2019 DICINT/CGI/DIP/PF
SPOOFING II					
ALVO	Equipe	Item	Laudo	Descrição	RAMA
Luiz Henrique Molição	4	2	1785/2019	01 Aparelho celular identificado marca APPLE, modelo A1586, IMEI 352068064785513 - senha de desbloqueio 829786	35/2019 DICINT/CGI/DIP/PF
Luiz Henrique Molição	4	1	1820/2019	01 notebook identificado marca ACER, cor cinza, mod ASPIRE F5-573, número de série NXGJLAL00371933CF69501	42/2019 DICINT/CGI/DIP/PF





MJSP - POLÍCIA FEDERAL
DIRETORIA DE INTELIGÊNCIA POLICIAL
COORDENAÇÃO-GERAL DE INTELIGÊNCIA
Divisão de Contrainteligência Policial

Luiz Henrique Molição	4	3	1820/2019	01 Notebook identificado marca LENOVO, cor preta, modelo 80AC, número de série PE00PGTF	42/2019 DICINT/CG/DIP/PF
Thiago Eliezer Martins Santos	1	1	1773/2019	Um aparelho celular iPhone X, IMEI 354861090034924, cor prata, com capa de proteção azul, modelo n° MQAD2BZ/A, N/S F2LW98JXJCLJ, senha: 0000, localizado no quarto de THIAGO.	30/2019 DICINT/CG I/DIP/PF
Thiago Eliezer Martins Santos	1	2	1811/2019	Um relógio APPLE WATCH, preto, serial FHLQ7MGGG9J6	NÃO SE APLICA
Thiago Eliezer Martins Santos	1	3	1811/2019	Um HD SEAGATE S/N W931ST1E, 1 TB	CRIPTOGRAFADO
Thiago Eliezer Martins Santos	1	4	1811/2019	Um HD 500GB, S/N: WCC2EM789118 WD - WD5000AAKX, SATA/16MB Cache	36/2019 DICINT/CG/DIP/PF
Thiago Eliezer Martins Santos	1	5	1811/2019	Um Sandisk Ultra 30MB/s*, 4 GB, cores preta, vermelha e cinza	36/2019 DICINT/CG/DIP/PF
Thiago Eliezer Martins Santos	1	6	1811/2019	Um notebook lenovo, cor preta, modelo 6881, S/N: PEC F099, Lenovo IDEAPAD 7400 TOUCH	NÃO SE APLICA
Thiago Eliezer Martins Santos	1	7	1811/2019	Um notebook em más condições, sem bateria, S/N: D06Q4R1, cores vermelha e preto	NÃO SE APLICA
Thiago Eliezer Martins Santos	1	9	1811/2019	Um microchip com "adapter", com tamanho 32 GB	36/2019 DICINT/CG/DIP/PF
Thiago Eliezer Martins Santos	1	12	1811/2019	Um notebook DELL, cores cinza e preto, INSPIRON, S/N 2 COJYR2, Reg. Model P61F	CRIPTOGRAFADO
Thiago Eliezer Martins Santos	1	15	1811/2019	Um modem 4G, dispositivo c WIFI Vivo	NÃO SE APLICA
Thiago Eliezer Martins Santos	1	16	1811/2019	Um pendrive vermelho DT 101, 8GB	36/2019 DICINT/CG/DIP/PF
Thiago Eliezer Martins Santos	1	17	1775/2019	Um IPAD prata, modelo MGNV2BR/A, N/S DV6P700EG5V2, localizado no quarto da mãe de THIAGO.	37/2019 DICINT/CG/DIP/PF





MJSP - POLÍCIA FEDERAL
DIRETORIA DE INTELIGÊNCIA POLICIAL
COORDENAÇÃO-GERAL DE INTELIGÊNCIA
Divisão de Contraineligência Policial

Thiago Eliezer Martins Santos	1	10 / 11 e 14	1786/2019	(item 10) Um chip VIVO 4G 895506566239 00222050439, localizado no quarto de THIAGO. (item 11) Um chip Oi, 8955 312929 927888842, localizado no quarto de THIAGO. (item 14) Um chip da VIVO 4G 8955066363 9003584779, localizado no quarto de THIAGO.	NÃO SE APLICA
Thiago Eliezer Martins Santos (São Paulo)	3	3	1794/2019	Um telefone celular marca SAMSUNG, modelo DUOS SSN - I9192GSMH	27/2019 DICINT/CG I/DIP/PF
Thiago Eliezer Martins Santos (São Paulo)	3	14	1795/2019	Um telefone celular marca SAMSUNG, modelo DUOS IMEI 1: 357739061786895 IMEI 2: 357740061786893 s/n: RX1G50DPK3X sem a tampa traseira	38/2019 DICINT/CGI/DIP/PF
Thiago Eliezer Martins Santos (São Paulo)	3	8	1815/2019	Um notebook marca SAMSUNG, S/N HX0G9QED500861V, com carregador	41/2019 DICINT/CGI/DIP/PF
Thiago Eliezer Martins Santos (São Paulo)	3	9	1815/2019	Um HD marca SEAGATE s/n 5YX1GCYP	CRIPTOGRAFADO
Thiago Eliezer Martins Santos (São Paulo)	3	10	1815/2019	Um HD marca WD, sem o serial number aparente, com etiqueta 1227-B5N-AD F1 A3502FB	CRIPTOGRAFADO
Thiago Eliezer Martins Santos (São Paulo)	3	11	1815/2019	Dois HD de computador: - marca WD, 1TB, s/n WXP1A68K1278 na caixa com o pedido número 1255 da empresa DOUTOR HD e cliente THIAGO MARTINS SANTOS - SSD NVME 960 evo s/n S3ESNX0K122162Z	41/2019 DICINT/CGI/DIP/PF
Thiago Eliezer Martins Santos (São Paulo)	3	13	1815/2019	Um HD marca SEAGATE s/n NA8HXX10	CRIPTOGRAFADO
Empresa Financeira	2	1	1806/2019	Um HD Seagate, 1TB, S/N 6VP06P0Z	26/2019 DICINT/CGI/DIP/PF

Além de dispositivos eletrônicos de armazenamento de dados, também foram apreendidos diversos materiais físicos, tais como cartões bancários e boletos em nome de terceiros, máquinas de leitura de cartão de crédito/débito, chips de celulares, dentre outros, que






MJSP - POLÍCIA FEDERAL
DIRETORIA DE INTELIGÊNCIA POLICIAL
COORDENAÇÃO-GERAL DE INTELIGÊNCIA
Divisão de Contraineligência Policial

também foram submetidos a procedimento de exploração e análise com a finalidade de formalizar suas vinculações com a hipótese criminal sob exame.

Do mesmo modo, além da arrecadação de material durante a deflagração das duas fases da Operação Spoofing, foram solicitadas medidas de afastamento de sigilo telemático de e-mails vinculados aos investigados, bem como de dados armazenados em sistemas de arquivo em nuvem. Assim, elaborou-se relatórios de análise contendo a síntese das evidências e elementos obtidos, os quais serão mencionados na individualização das condutas de cada um dos investigados.

Por fim, deve ser mencionado o Laudo de Perícia Criminal Contábil-Financeiro nº 2161/2019-INC/DITEC/PF, que analisou dados bancários relacionado às 06 (seis) pessoas físicas e 01 (uma) pessoa jurídica, que constam das decisões de afastamento de sigilo bancário listadas na tabela abaixo:

CPF/CNPJ	Nome	Período de quebra
17.599.733/0001-97	AME RESTAURANTE LTDA	01/01/2018 a 31/12/2018
370.074.428-54	DANILO CRISTIANO MARQUES	01/01/2018 a 17/07/2019
389.864.308-51	GUSTAVO HENRIQUE ELIAS SANTOS	01/01/2018 a 17/07/2019
498.486.768-05	LUIZ HENRIQUE MOLIÇÃO	01/01/2019 a 17/07/2019
427.742.138-51	SUELEN PRISCILA DE OLIVEIRA	01/01/2018 a 17/07/2019
026.158.451-01	THIAGO ELIEZER MARTINS SANTOS	01/01/2018 a 17/07/2019
378.676.428-03	WALTER DELGATTI NETO	01/01/2018 a 17/07/2019

Com relação às movimentações bancárias no ano de 2018, referentes a DANILO CRISTIANO MARQUES, GUSTAVO HENRIQUE ELIAS SANTOS, SUELEN PRISCILA DE OLIVEIRA e WALTER DELGATTI NETO, será elaborado laudo complementar após a transmissão completa dos dados bancários por parte das instituições financeiras. Por sua vez, as movimentações financeiras abordadas no Laudo Contábil-Financeiro nº 2161/2019-INC/DITEC/PF, e que sejam do interesse das investigações, serão mencionadas na descrição das hipóteses criminais sob apuração, bem como na contextualização e individualização das condutas de cada investigado.





MJSP - POLÍCIA FEDERAL
DIRETORIA DE INTELIGÊNCIA POLICIAL
COORDENAÇÃO-GERAL DE INTELIGÊNCIA
Divisão de Contraineligência Policial

Seguem abaixo as principais evidências reunidas, organizadas de forma individualizada em relação a cada um dos investigados.

9 – CRIMES APURADOS

A presente investigação criminal tem por objetivo final realizar o enquadramento legal dos dados apurados, atribuindo o tipo penal aos eventos que chegaram ao conhecimento da Polícia Federal. Assim, o trabalho de preparação dos enunciados fáticos que serão submetidos ao Ministério Público Federal e ao Poder Judiciário somente é possível mediante a análise de crimes específicos, com a consequente subsunção dos eventos à norma.

O sentido legal dos fatos em apuração é obtido a partir dos tipos penais que lhes conferem relevância criminal. Por sua vez, tendo em vista a multiplicidade de eventos que compõem o fluxo temporal da presente investigação criminal, devem ser ressaltados apenas os elementos que possuem relevância jurídica para cada crime específico. Assim, as evidências reunidas no curso do presente Inquérito Policial serão apresentadas de acordo com o tipo penal a que estão vinculadas e que servem como elemento de corroboração.

Entretanto, deve ser ressaltado que, por óbvio, a captulação realizada em sede policial não vincula o titular da ação penal, podendo o membro do Ministério Público adequar ou complementar o enquadramento jurídico dos fatos, conforme outros entendimentos levando em consideração.

9.1 - ORGANIZAÇÃO CRIMINOSA

Os fatos investigados no presente Inquérito Policial foram apresentados de em linguagem coloquial pela imprensa como sendo ações de “hackers”, termo importado da língua inglesa e que pode ser traduzido por decifrador. Por sua vez, o verbo “hackear” costuma ser usado para descrever modificações e manipulações não autorizadas em sistemas de computação. Assim, os hackers, de uma forma geral, seriam programadores de computadores habilidosos, em sua maioria jovens estudantes, e por dedicarem muito tempo a





MJSP - POLÍCIA FEDERAL
DIRETORIA DE INTELIGÊNCIA POLICIAL
COORDENAÇÃO-GERAL DE INTELIGÊNCIA
Divisão de Contraineligência Policial

pesquisa e experimentação, possuiriam reduzida atividade social e se encaixariam no estereótipo do chamado “nerd”.

Entretanto, a palavra “*hacker*” também pode ser associada ao chamado criminoso virtual, sendo esta a definição correta a ser aplicada nesta investigação criminal. Na realização de crimes virtuais, muitos *hackers* compartilham informações e colaboram em ações em comum, de acordo com a habilidade demonstrada por cada um. Em alguns casos, esta colaboração entre os criminosos pode ocorrer apenas de modo virtual, sendo também comum a utilização de codinomes (*nicknames*) para serem identificados em *chats* na internet ou em grupos de aplicativo de comunicação.

Neste sentido, foram encontrados diálogos realizadas por WALTER DELGATTI NETO através do aplicativo “Skype” (usuário Skype goextremehardorgohome), que versavam, em sua maioria, sobre fraudes bancárias, bem como registros de conversas por meio do programa “Adium 2.0” com conteúdo semelhante. Segundo o Laudo nº 1458/2109-INC/DITEC/PF (fls. 435/440), essas conversas foram realizadas partir de tal programa utilizando os protocolos *Internet Relay Chat* (IRC) e (ICQ).

A análise dos referidos diálogos, materializada no RAMA 04/2019, traz um quadro do funcionamento do submundo do crime virtual, com a intensa comercialização de informações e instrumentos para a prática dos crimes em grupos e *chats* especializados, conforme os exemplos a seguir:

i) “Toguro vendas CC ON”: neste grupo de mensagens, as conversas são claras e objetivas. Os integrantes, inclusive WALTER NETO, que utiliza o usuário “goextremehardorgohome”, negociam a venda de cartões de créditos em nome de terceiros e *malwares*, solicitam e oferecem informações sobre placas de veículos, pessoas físicas e outros serviços. Trata-se, efetivamente, de um grupo de comércio, inclusive com ofertas e promoções, praticados por criminosos. Segue trecho das extensas mensagens verificadas neste grupo:





ii) Grupo "WOrk": *chat* com finalidade similar ao anterior, que conta também com o suporte de WALTER NETO:

iii) “Xímia__CdD”: foram registradas conversas entre o usuário “ximiapriv8” e WALTER NETO, que se identificava como PAULO MENDES (nickname2 goextremehardorgohome). O interlocutor de WALTER inicia a conversa oferecendo “infect” 3. WALTER, em resposta, afirma que necessitará atualizar a “kl” 4, e complementa “mas vou precisar de *infect* sim”. Logo após, WALTER pergunta sobre o valor do *infect* oferecido, referência a softwares maliciosos, bem como cartões de créditos. Num determinado momento da conversa, “ximiapriv8” afirma que eles já fizeram “negócio” antes, tendo WALTER afirmado ter depositador R\$ 1.400,00 “de cc5 acho”:





MJSP - POLÍCIA FEDERAL
DIRETORIA DE INTELIGÊNCIA POLICIAL
COORDENAÇÃO-GERAL DE INTELIGÊNCIA
Divisão de Contrainteligência Policial

1517	25/05/2018	22 14 51	atrasado	gratuitamente do governo. E se não
1518	25/05/2018	22 14 51	atrasado	gratuitamente do governo. E se não, de onde é melhor eu
1519	25/05/2018	22 14 51	atrasado	gratuitamente do governo. E se não
1520	25/05/2018	22 14 51	atrasado	gratuitamente do governo. E se não
1521	25/05/2018	22 14 51	atrasado	gratuitamente do governo. E se não
1522	25/05/2018	22 14 51	atrasado	gratuitamente do governo. E se não
1523	25/05/2018	22 14 51	atrasado	gratuitamente do governo. E se não
1524	25/05/2018	22 14 51	atrasado	gratuitamente do governo. E se não
1525	25/05/2018	22 14 51	atrasado	gratuitamente do governo. E se não
1526	25/05/2018	22 14 51	atrasado	gratuitamente do governo. E se não
1527	25/05/2018	22 14 51	atrasado	gratuitamente do governo. E se não
1528	25/05/2018	22 14 51	atrasado	gratuitamente do governo. E se não
1529	25/05/2018	22 14 51	atrasado	gratuitamente do governo. E se não
1530	25/05/2018	22 14 51	atrasado	gratuitamente do governo. E se não
1531	25/05/2018	22 14 51	atrasado	gratuitamente do governo. E se não
1532	25/05/2018	22 14 51	atrasado	gratuitamente do governo. E se não
1533	25/05/2018	22 14 51	atrasado	gratuitamente do governo. E se não
1534	25/05/2018	22 14 51	atrasado	gratuitamente do governo. E se não
1535	25/05/2018	22 14 51	atrasado	gratuitamente do governo. E se não
1536	25/05/2018	22 14 51	atrasado	gratuitamente do governo. E se não
1537	25/05/2018	22 14 51	atrasado	gratuitamente do governo. E se não
1538	25/05/2018	22 14 51	atrasado	gratuitamente do governo. E se não
1539	25/05/2018	22 14 51	atrasado	gratuitamente do governo. E se não
1540	25/05/2018	22 14 51	atrasado	gratuitamente do governo. E se não
1541	25/05/2018	22 14 51	atrasado	gratuitamente do governo. E se não
1542	25/05/2018	22 14 51	atrasado	gratuitamente do governo. E se não
1543	25/05/2018	22 14 51	atrasado	gratuitamente do governo. E se não
1544	25/05/2018	22 14 51	atrasado	gratuitamente do governo. E se não
1545	25/05/2018	22 14 51	atrasado	gratuitamente do governo. E se não
1546	25/05/2018	22 14 51	atrasado	gratuitamente do governo. E se não
1547	25/05/2018	22 14 51	atrasado	gratuitamente do governo. E se não
1548	25/05/2018	22 14 51	atrasado	gratuitamente do governo. E se não

iv) "IGR": o usuário "igr.gov" foi repassado pelo "Ximia_CdD", reportado no item 3.1.4, como o contato para vender dados de clientes do Banco do Brasil a WALTER. O interlocutor "igr.gov" afirma ter "123 BB" para vender, inclusive com senhas de 4 dígitos, por "2500\$". WALTER questiona se ele tem o "plástico"6 ou a "info" e afirma possuir a URA (Unidade de Resposta Audível) de todos os bancos, informando que tem o interesse em comprar "plástico". Estas gravações, utilizadas pelos bancos em seus atendimentos automatizados (URA), foram, de fato, encontradas em um *pendrive* (item 3 do auto de apreensão) que estava em posse de WALTER:

1549	25/05/2018	22 14 51	atrasado	gratuitamente do governo. E se não
1550	25/05/2018	22 14 51	atrasado	gratuitamente do governo. E se não
1551	25/05/2018	22 14 51	atrasado	gratuitamente do governo. E se não
1552	25/05/2018	22 14 51	atrasado	gratuitamente do governo. E se não
1553	25/05/2018	22 14 51	atrasado	gratuitamente do governo. E se não
1554	25/05/2018	22 14 51	atrasado	gratuitamente do governo. E se não
1555	25/05/2018	22 14 51	atrasado	gratuitamente do governo. E se não
1556	25/05/2018	22 14 51	atrasado	gratuitamente do governo. E se não
1557	25/05/2018	22 14 51	atrasado	gratuitamente do governo. E se não
1558	25/05/2018	22 14 51	atrasado	gratuitamente do governo. E se não
1559	25/05/2018	22 14 51	atrasado	gratuitamente do governo. E se não
1560	25/05/2018	22 14 51	atrasado	gratuitamente do governo. E se não
1561	25/05/2018	22 14 51	atrasado	gratuitamente do governo. E se não
1562	25/05/2018	22 14 51	atrasado	gratuitamente do governo. E se não
1563	25/05/2018	22 14 51	atrasado	gratuitamente do governo. E se não
1564	25/05/2018	22 14 51	atrasado	gratuitamente do governo. E se não
1565	25/05/2018	22 14 51	atrasado	gratuitamente do governo. E se não
1566	25/05/2018	22 14 51	atrasado	gratuitamente do governo. E se não
1567	25/05/2018	22 14 51	atrasado	gratuitamente do governo. E se não
1568	25/05/2018	22 14 51	atrasado	gratuitamente do governo. E se não
1569	25/05/2018	22 14 51	atrasado	gratuitamente do governo. E se não
1570	25/05/2018	22 14 51	atrasado	gratuitamente do governo. E se não
1571	25/05/2018	22 14 51	atrasado	gratuitamente do governo. E se não
1572	25/05/2018	22 14 51	atrasado	gratuitamente do governo. E se não
1573	25/05/2018	22 14 51	atrasado	gratuitamente do governo. E se não
1574	25/05/2018	22 14 51	atrasado	gratuitamente do governo. E se não
1575	25/05/2018	22 14 51	atrasado	gratuitamente do governo. E se não
1576	25/05/2018	22 14 51	atrasado	gratuitamente do governo. E se não
1577	25/05/2018	22 14 51	atrasado	gratuitamente do governo. E se não
1578	25/05/2018	22 14 51	atrasado	gratuitamente do governo. E se não
1579	25/05/2018	22 14 51	atrasado	gratuitamente do governo. E se não
1580	25/05/2018	22 14 51	atrasado	gratuitamente do governo. E se não





MJSP - POLÍCIA FEDERAL
DIRETORIA DE INTELIGÊNCIA POLICIAL
COORDENAÇÃO-GERAL DE INTELIGÊNCIA
Divisão de Contraineligência Policial

v) Chat "João Estrela": na conversa WALTER e o interlocutor joaopestrela100 afirma que consegue ligar para as vítimas através do número do próprio banco. Esta manipulação do número chamador também foi utilizada para acessar os correios de voz das vítimas e ouvir o código enviado pelo *Telegram*. A mensagem em que WALTER afirma ligar do número do banco é de 19/06/2018 e a conta ID 34221 da BRVOZ, principal conta utilizada nas invasões, foi criada em 22/06/2019. Este cenário poderia sugerir que WALTER já utilizava este mecanismo de manipular o número chamado antes até da criação da conta ID 34221 na BRVOZ:

7077	19/06/2018 17:56:50	gustavomartins@guilherme	seu proprio banco	seu proprio banco
7078	19/06/2018 17:56:48	gustavomartins@guilherme	seu proprio banco	seu proprio banco
7079	19/06/2018 17:56:48	gustavomartins@guilherme	seu proprio banco	seu proprio banco
7080	19/06/2018 17:56:48	gustavomartins@guilherme	seu proprio banco	seu proprio banco
7081	19/06/2018 17:56:48	gustavomartins@guilherme	seu proprio banco	seu proprio banco
7082	19/06/2018 17:56:48	gustavomartins@guilherme	seu proprio banco	seu proprio banco
7083	19/06/2018 17:56:48	gustavomartins@guilherme	seu proprio banco	seu proprio banco
7084	19/06/2018 17:56:48	gustavomartins@guilherme	seu proprio banco	seu proprio banco
7085	19/06/2018 17:56:48	gustavomartins@guilherme	seu proprio banco	seu proprio banco
7086	19/06/2018 17:56:48	gustavomartins@guilherme	seu proprio banco	seu proprio banco
7087	19/06/2018 17:56:48	gustavomartins@guilherme	seu proprio banco	seu proprio banco
7088	19/06/2018 17:56:48	gustavomartins@guilherme	seu proprio banco	seu proprio banco
7089	19/06/2018 17:56:48	gustavomartins@guilherme	seu proprio banco	seu proprio banco
7090	19/06/2018 17:56:48	gustavomartins@guilherme	seu proprio banco	seu proprio banco
7091	19/06/2018 17:56:48	gustavomartins@guilherme	seu proprio banco	seu proprio banco
7092	19/06/2018 17:56:48	gustavomartins@guilherme	seu proprio banco	seu proprio banco
7093	19/06/2018 17:56:48	gustavomartins@guilherme	seu proprio banco	seu proprio banco
7094	19/06/2018 17:56:48	gustavomartins@guilherme	seu proprio banco	seu proprio banco
7095	19/06/2018 17:56:48	gustavomartins@guilherme	seu proprio banco	seu proprio banco
7096	19/06/2018 17:56:48	gustavomartins@guilherme	seu proprio banco	seu proprio banco

9.1.1 – GRUPO DE ARARAQUARA

A associação criminosa investigada possui um grupo inicial específico que foi formado na cidade de Araraquara/SP, composto por WALTER DELGATTI NETO, GUSTAVO HENRIQUE ELIAS SANTOS, SUELEN PRISCILA DE OLIVEIRA e DANILO CRISTIANO MARQUES, os quais possuíam histórico de crimes praticados em conjunto.

Segundo a Informação nº 076/2018 – DFIN/DICOR/PF, foi verificado que WALTER DELGATTI NETO, também conhecido pela alcunha "VERMELHO", responderia na Justiça de São Paulo pelos seguintes crime:





MJSP - POLÍCIA FEDERAL
DIRETORIA DE INTELIGÊNCIA POLICIAL
COORDENAÇÃO-GERAL DE INTELIGÊNCIA
Divisão de Contraineligência Policial

Foro de Araraquara:

i) 0013971-19.2015.8.26.0037
Ação Penal - Procedimento Ordinário / Furto Qualificado
Réu: Walter Delgatti Neto
Recebido em: 07/12/2015 - 1ª Vara Criminal

ii) 0004334-44.2015.8.26.0037
Ação Penal - Procedimento Ordinário / Tráfico de Drogas e Condutas Afins
Réu: Walter Delgatti Neto
Recebido em: 16/04/2015 - 3ª Vara Criminal

iii) 0018495-30.2013.8.26.0037
Ação Penal - Procedimento Ordinário / Crimes contra o Patrimônio
Réu: Walter Delgatti Neto
Recebido em: 26/07/2013 - 1ª Vara Criminal

Foro de Ribeirão Preto

iv) 0013056-57.2011.8.26.0506 (412/2011)
Ação Penal - Procedimento Ordinário / Estelionato
Réu: Walter Delgatti Neto
Recebido em: 15/03/2011 - 5ª Vara Criminal

Foro de Rio Claro

v) 0016724-87.2012.8.26.0510 (510.01.2012.016724)
Ação Penal - Procedimento Ordinário / Estelionato
Réu: Walter Delgatti Neto
Recebido em: 11/10/2012 - 1ª Vara Criminal

WALTER DELGATTI NETO também responderia ao seguinte processo criminal perante a Justiça Santa Catarina:

vi) 0001229-80.2015.8.24.0048
Classe: Termo Circunstanciado
Área: Criminal 2ª Vara criminal – Balneário Piçarras/SC
Assunto: Uso de documento falso





MJSP - POLÍCIA FEDERAL
DIRETORIA DE INTELIGÊNCIA POLICIAL
COORDENAÇÃO-GERAL DE INTELIGÊNCIA
Divisão de Contraineligência Policial

Ressalte-se, também, que no momento da deflagração da Operação Spoofing WALTER DELGATTI NETO se encontrava evadido da justiça, motivo pelo qual utilizava imóvel alugado em nome de DANILO CRISTIANO MARQUES para se esconder dos órgãos policiais encarregados do cumprimento do mandado de prisão expedido pela 1ª Vara Criminal da Comarca de Araraquara/SP, referente ao processo nº 0013971-19.2015.8.26.0037 que condenou WALTER NETO em sentença definitiva pelo cometimento de crime contra o patrimônio.

Em pesquisas realizadas no Cadastro Nacional de Informações Sociais – CNIS, não foi encontrado qualquer vínculo formal de trabalho em nome de WALTER DELGATTI NETO. Entretanto, verificou-se no material apreendido inúmeros registros de imagens em que WALTER DELGATTI NETO ostenta sinais incompatíveis de riqueza, como as que foram registradas na Informação nº 50/2019-DICINT/CGI/DIP/PF:



Por sua vez, existem diversas evidências que indicam a participação de WALTER DELGATTI NETO na realização sistemática de fraudes bancárias. Como exemplo, pode-se citar o arquivo denominado “*envia.php*”, encontrado na pasta raiz do computador de WALTER NETO, que seria utilizado para carregar a página “*eng.html*” a sugerir um tipo de ataque conhecido no meio cibernético como *phishing*, técnica de fraude *on line* utilizada por criminosos para roubar senhas de bancos e demais informações de vítimas:





MJSP - POLÍCIA FEDERAL
DIRETORIA DE INTELIGÊNCIA POLICIAL
COORDENAÇÃO-GERAL DE INTELIGÊNCIA
Divisão de Contrainteligência Policial



Ainda segundo a Informação nº 29/2019-DICINT/CGI/DIP, o arquivo "UNADJUSTEDNONRAW_thumb_1e2f.jpeg", também localizado no computador WALTER DELGATTI NETO, apresenta conversas de interlocutores em que são repassadas informações que aparentam ser de cartões de possíveis vítimas, conforme imagem abaixo:



Também foram verificados elementos de prova que demonstram ser WALTER DELGATTI NETO um especialista na aplicação de técnicas de engenharia social, possuindo forte poder de persuasão para obter informações que são utilizadas para o acesso não autorizado a sistemas de computadores.

[Assinatura manuscrita]





MJSP - POLÍCIA FEDERAL
DIRETORIA DE INTELIGÊNCIA POLICIAL
COORDENAÇÃO-GERAL DE INTELIGÊNCIA
Divisão de Contrainteligência Policial

Segundo a Informação nº 50/2019-DICINT/CGI/DIP/PF, foi encontrado no e-mail tadanado@icloud.com, que era utilizado por WALTER DELGATTI NETO, o arquivo de uma gravação de áudio na qual WALTER NETO se apresenta como sendo o responsável pela área técnica de segurança de determinada instituição financeira e orienta uma cliente do banco, de nome FERNANDA, a efetuar a atualização do computador, provavelmente para instalação de programa malicioso para captura de senhas e dados bancários. Na gravação é possível ouvir barulhos de teclado, o que seria uma estratégia de WALTER para imitar uma central de atendimento bancário.

FERNANDA: oi.

WALTER: oi, pois não senhora.

FERNANDA: heim FERNANDO aqui tem muita... tem muito hacker... sei lá esses trem a gente fica meio com medo

WALTER: ah sim!

....

WALTER: agora a senhora faz o acesso, conta corrente, consultas e tira o extrato. Automaticamente ele vai começar novamente a atualização.

FERNANDA: e, aí eu tenho que fazer nas minhas duas empresas essa atualização?

WALTER: acredito que sim senhora, porém, o meu contato é pra fazer nessa empresa! A outra empresa da senhora... só um minuto, deixa eu vê se eu tenho acesso aqui... a outra é Loucuras de Amor né?

FERNANDA: Isso.

WALTER: Ah sim! Acredito que a senhora receberá um novo contato para fazer a atualização na outra. Porém, com esse contato a senhora já toma conhecimento de como faz e pode fazer sozinha senhora.

FERNANDA: ah tá! Não porque, realmente é..., assim pediu várias vezes para fazer isso, só que foi esquecendo

WALTER: ah sim...

FERNANDA: eu fiquei achando que era hacker, vírus, alguma coisa. Então tinha pedido esse mesmo procedimento aí, só que eu não deixava finalizar, que eu tava com medo

WALTER: ah entendi

FERNANDA: eu esqueci de ligar pro meu gerente entendeu?

WALTER: entendi





MJSP - POLÍCIA FEDERAL
DIRETORIA DE INTELIGÊNCIA POLICIAL
COORDENAÇÃO-GERAL DE INTELIGÊNCIA
Divisão de Contrainteligência Policial

FERNANDA: pra verificar com ele

WALTER: ah... mas como ele autorizou agora tudo bem! É como eu te disse senhora por esse motivo que a senhora não fez antes, hoje é o último dia né... no caso do prazo

FERNANDA: entendi.

WALTER: por esse motivo a senhora teria de fazer hoje porque se esperasse até segunda feira só seria possível com um técnico indo até a empresa da senhora. Isso demora até sete dias úteis e a senhora poderia ficar sem acesso a conta on line por sete dias

FERNANDA: ah entendi...

FERNANDA: FERNANDO, apareceu aqui pra eu digitar uma senha

WALTER: é a senha do certificado né.

FERNANDA: isso.

WALTER: a senhora digita a senha, não me informe tá senhora!

FERNANDA: oi?

WALTER: a senhora digita a senha não me informe ela tá!

FERNANDA: ok.

FERNANDA: e aí, e agora qual que vai ser o procedimento na hora que reiniciar?

WALTER: senhora, agora com a finalização, o seu computador faz o reiniciamento e, logo em seguida, a senhora tem acesso normal à sua conta como antes

FERNANDA: aí vai mudar é... o... banco tá mudando? Assim é... a forma de trabalhar, como é que é? O que que é...

WALTER: na realidade o design do banco não afeta em nada, porém, esse guardião, ele defende as movimentações da sua conta e acessos irregulares feitos por terceiros. Caso aconteça um acesso que não é da senhora, exemplo, num outro computador, na hora, automaticamente ele manda uma notificação pro seu gerente e o seu gerente entra em contato com a senhora, confirmando se realmente foi a senhora que fez esse acesso ou não. Caso não foi a senhora ele faz um bloqueio preventivo da sua conta, entendeu senhora?

FERNANDA: ahm... entendi.

WALTER: ele na realidade é um guardião mesmo, ele toma conta da sua conta. Caso seja feito algum pagamento, alguma transferência que não é da senhora automaticamente ele faz o bloqueio da transferência, do pagamento, entra em contato com o seu gerente e aguarda uma autorização dele. Caso ele fale: não, realmente foi minha cliente ele faz a liberação, caso não, ele faz o bloqueio e a senhora nunca será lesada com isso, com esse guardião...

WALTER: olha senhora, aqui no sistema já consta como finalizado, ele vai reiniciar aí e eu agradeço a sua atenção...





MJSP - POLÍCIA FEDERAL
DIRETORIA DE INTELIGÊNCIA POLICIAL
COORDENAÇÃO-GERAL DE INTELIGÊNCIA
Divisão de Contraineligência Policial

FERNANDA: mais eu tô fazendo aqui, ele falou assim: "não FERNANDA pode..." ele me ligou, que tava passando whatsapp pra ele e ele me ligou e falou, "não FERNANDA pode fazer que sem isso não tem problema"

WALTER: não tudo bem, como eu te disse, eu não vou confirmar nada com a senhora, agora a senhora fica tranquila né!

FERNANDA: ah é, porque sei lá...

WALTER: Não! É normal.

FERNANDA: É normal né?

WALTER: Isso senhora!

FERNANDA: Ruim é quando a pessoa vai fazendo sem falar nada né?

WALTER: Não, com certeza é até bom a senhora sempre procurar um gerente, coisa do tipo, aí a senhora fica mais segura né?

FERNANDA: anh ham...

Em outro arquivo de áudio, que também foi encontrado no e-mail tadanado@icloud.com, WALTER NETO, novamente passando-se por responsável de área técnica bancária, orienta e tenta persuadir o cliente, homem não identificado (HNI), a efetuar a atualização de software do computador, provavelmente também com o intuito de instalar programa malicioso para captura de senhas e dados bancários. Segue abaixo transcrição de partes relevantes do áudio:

WALTER: acontece o seguinte senhor...

HNI: agora eu tenho uma gerente que não me liga pra nada e eu não sei nada do que acontece, quando eu ligo lá não atende o telefone

WALTER: é

HNI: eu tô mal assessorado

WALTER: é por esse motivo que a gente tem uma central específica pra resolver isso

HNI: anh ham

WALTER: senhor acontece o seguinte: como o senhor havia dito, toda vez que começa atualização acontece alguma fraude na conta do senhor. Porém, como o senhor disse: o vagabundo né, ele usa a atualização do banco que existe como uma desculpa para pode fazer também a atualização, entendeu senhor?

HNI: anh ham





MJSP - POLÍCIA FEDERAL
DIRETORIA DE INTELIGÊNCIA POLICIAL
COORDENAÇÃO-GERAL DE INTELIGÊNCIA
Divisão de Contraineligência Policial

WALTER: por esse motivo que o banco também atualiza, o banco atualiza e o vagabundo também senhor

HNI: não eu entendi, mais, mais...é que é assim... só pra você entender o meu ponto de vista

WALTER: sim

HNI: eu tô com um dinheiro lá na conta e eu preciso pagar um boleto hoje, eu preciso usar o dinheiro hoje, cê entendeu? Aí quando eu vi que que entrou essa merda dessa atualização

WALTER: entendi

HNI: e eu não tô sabendo de nada, minha gerente não me fala nada, não sabe nada, pra mim é alguém querendo hackear a minha conta

WALTER: ah entendi

HNI: aí eu peguei e fui lá e desliguei tudo, cê entendeu?

WALTER: é que essa atualização está sendo feita em todos os computadores, em todas as contas

HNI: não, positivo. Isso Você tá me falando, só que assim, a minha gerente nunca me falou nada que tem que fazer atualização e tem isso, tem aquilo e aquilo outro

WALTER: com certeza!

HNI: quando eu vi acontecendo isso e, e... foi semelhante ao que aconteceu da outra vez eu desliguei tudo

WALTER: não, com certeza

HNI: eu vou falar meu, eu vou me ferrar aqui, eu vou perder onze conto, o banco vai demorar uma semana pra me devolver o dinheiro e eu não consigo mais pagar as minhas contas

WALTER: entendi senhor, mas dessa vez não é fraude senhor!

A conversa continua com HNI pedindo o telefone de contato da central de atendimento para WALTER DELGATTI NETO, que é identificado pelo nome de FERNANDO. WALTER informa os supostos telefones de contato para HNI e diz aguardar pela ligação.

Demonstrando ainda sua habilidade em praticar crimes valendo-se de técnicas de engenharia social, em outra gravação WALTER NETO se passa por empregado da área de segurança do banco Santander e liga para o gerente de uma agência da instituição com o objetivo de descobrir os procedimentos internos do banco, conforme RAMA nº 4/DICINT/CGI/DIP/PF.





MJSP - POLÍCIA FEDERAL
DIRETORIA DE INTELIGÊNCIA POLICIAL
COORDENAÇÃO-GERAL DE INTELIGÊNCIA
Divisão de Contrainteligência Policial

Também foi encontrado no e-mail gutodubra@icloud um vídeo em que GUSTAVO HENRIQUE filma WALTER NETO realizando uma ligação para uma possível vítima de fraude bancária. Seguem imagem e transcrição do arquivo IMG_1041.mov:



WALTER: Senhora, a senhora está no [inaudível] melhor né?!

WALTER: A senhora colocou o "www"?

Ressalte-se que a capacidade demonstrada por WALTER NETO de improvisar histórias, conforme as diversas gravações de golpes que foram encontradas no material probatório reunido, foi também percebida durante as suas oitivas realizadas ao longo da investigação, reforçando a necessidade da Polícia Federal de se basear em exames periciais e provas materiais para realizar a reconstituição fidedigna dos fatos ocorridos.





MJSP - POLÍCIA FEDERAL
DIRETORIA DE INTELIGÊNCIA POLICIAL
COORDENAÇÃO-GERAL DE INTELIGÊNCIA
Divisão de Contraineligência Policial

Conforme Relatório de Análise Bancária nº 01/2019/NO/DICINT/CGI/DIP/PF, WALTER DELGATTI NETO movimentou, no período de 08/06/2019 a 04/12/2018, em operações registradas no banco NU o total bruto (sem expurgos) de R\$ 46.664,45 (créditos). As movimentações referentes ao período de 01/01/2019 a 17/07/2019 foram lançadas Laudo nº 2161/2019, ressaltando-se que WALTER DELGATTI NETO utilizava contas em nome de DANILO CRISTIANO para realizar transferências bancárias:

Ano	Créditos (R\$)			Débitos (R\$)		
	Brutos	Expurgos	Líquidos	Brutos	Expurgos	Líquidos
2019	107.702,54	26.350,00	81.352,54	116.055,07	26.350,00	89.705,07

Por sua vez, em relação a GUSTAVO HENRIQUE ELIAS SANTOS foram localizados em bancos de dados da Secretaria de Segurança Pública do Estado de São Paulo vários registros criminais referentes aos crimes de ameaça, falsificação de documentos, receptação, uso de documento falso e furto, além da prisão em flagrante ocorrida em 2015 após GUSTAVO HENRIQUE ter sido encontrado pela Polícia Militar portando um revólver calibre 357, juntamente com 5 cartuchos intactos, conforme a Informação nº 023/19 – DICINT/CGI/DIP/PF:

- i) IPL 23/2013 - D.P. Araraquara. Tipo: Flagrante por falsificação de documento público e utilização de papéis falsificados (Art. 297 e 304 do CP);
- ii) IPL 094/2014 - D. P. Panorama. Tipo: Portaria. Furto (art. 155).
- iii) IPL 023/2015 - D. S. Taboão da Serra. Tipo: Flagrante. Porte ilegal de arma de fogo.
- iv) Ação Penal nº 966/2013 - Vara Criminal de Araraquara. Denunciado por adulteração de chassi (art. 311 CP), fazer uso de papéis falsificados (art. 304 CP) e alterar documento público (art. 297). Sentença: Condenado. Pena: 6 anos em regime semiaberto.

Existem inúmeros elementos de prova indicando que GUSTAVO HENRIQUE ELIAS SANTOS possui atividades criminais cotidianas. Conforme Relatório de Análise de Conteúdo em Nuvem nº 001/2019 SOI/DICINT/CGI/DIP e Informação nº 49/2019/DICINT/CGI/DIP, foram encontrados nos e-mails gutodubra@icloud.com e





MJSP - POLÍCIA FEDERAL
DIRETORIA DE INTELIGÊNCIA POLICIAL
COORDENAÇÃO-GERAL DE INTELIGÊNCIA
Divisão de Contrainteligência Policial

djgutodubra@icloud.com diversos arquivos de foto e vídeos em que o investigado ostenta dinheiro e outros recursos obtidos de forma ilícita. Seguem abaixo alguns exemplos:



Transcrição do áudio vinculado ao vídeo:

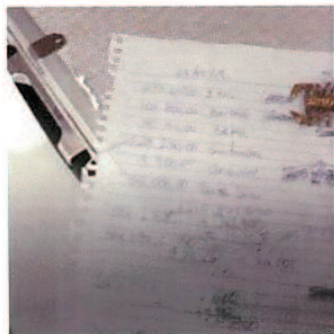
GUSTAVO: Bom dia grupo! Vamo focar, vamo focar no golpe.

Em outro vídeo mencionado no Relatório de Análise de Conteúdo em Nuvem nº 001/2019, GUSTAVO HENRIQUE conta quantia em espécie através de uma máquina de contar cédulas e filma uma folha de papel onde anota a contabilidade de 27/03/2019. Das anotações contábeis depreende-se: 245.640,00 (Itaú), 102.800,00 (Bradesco), 70.450,00 (Brasil), 129.250,00 (Santander), 19.900,00 (Original), 55.000,00 (Western Union):





MJSP - POLÍCIA FEDERAL
DIRETORIA DE INTELIGÊNCIA POLICIAL
COORDENAÇÃO-GERAL DE INTELIGÊNCIA
Divisão de Contraineligência Policial



O investigado também realizou uma filmagem em que desembala grande quantia de dinheiro, explicando que alguém teria enviado as notas de forma a ocultá-las em embalagens de macarrão, torradas, sacolas plásticas:



Transcrição Vídeo

GUTO: Ele manda assim, em sacolinha de... ou é caixa ou é, ou é sacola de pão, de macarrão, de arroz.

Em outro vídeo, feito no interior de um veículo, GUSTAVO revela que estaria transportando grande quantia de dinheiro para Ribeirão Preto:





MJSP - POLÍCIA FEDERAL
DIRETORIA DE INTELIGÊNCIA POLICIAL
COORDENAÇÃO-GERAL DE INTELIGÊNCIA
Divisão de Contraineligência Policial



Transcrição (IMG 3100)

GUTO: Ô viado, tô indo pra porra de Ribeirão Preto. Olha aqui fio, não tem nem onde... não cabe mais dinheiro. Oh, oh.

Guto abre o console do veículo e mostra os maços de nota.

GUTO: Ô o que eu tô tendo que fazer aqui. Fora o banco de trás. Não tem, não tem... vai vai segurando essa porra aí, veado. Ô, não dá nem pra fechar a mão mano. Tá chapando?

Também foram encontrados vídeos e fotos em que GUSTAVO HENRIQUE expõe a posse de armas de fogo:





MJSP - POLÍCIA FEDERAL
DIRETORIA DE INTELIGÊNCIA POLICIAL
COORDENAÇÃO-GERAL DE INTELIGÊNCIA
Divisão de Contraineligência Policial

Também foram mencionadas na Informação nº 49/2019/DICINT/CGI/DIP imagens e vídeos que evidenciaram o envio e recebimento, por GUSTAVO HENRIQUE, de cartões bancários pelos Correios:



Conforme Relatório de Análise Bancária nº 01/2019/NO/DICINT/CGI/DIP/PF, GUSTAVO HENRIQUE ELIAS SANTOS movimentou, no período de 08/06/2019 a 04/12/2018, em operações no Banco Inter S/A, Banco Original, Banco do Brasil e Caixa Econômica Federal o total bruto (sem expurgos) de R\$ 1.063.955,62 (créditos).

Por sua vez, segundo o Laudo Contábil-Financeiro nº 2161/2019, GUSTAVO HENRIQUE ELIAS SANTOS movimentou, no período de 01/01/2019 a 17/07/2019, os valores mencionados na tabela abaixo:

GUSTAVO HENRIQUE ELIAS SANTOS (389.864.308-51)						
Ano	Créditos (R\$)			Débitos (R\$)		
	Brutos	Expurgos	Líquidos	Brutos	Expurgos	Líquidos
2019	440.826,78	273.802,67	167.024,11	471.762,58	169.660,00	302.102,58

Em suas atividades ilícitas, GUSTAVO HENRIQUE contaria com a participação e cumplicidade de SUELEN PRISCILA DE OLIVEIRA, tendo sido encontrado no imóvel ocupado pelo casal farto material indicativo do cometimento de crimes e fraudes bancárias em diversas modalidades, tais como cartões bancários e boletos em nome de terceiros, além de diversas máquinas de leitura de cartão de crédito/débito. Do mesmo modo, foi





MJSP - POLÍCIA FEDERAL
DIRETORIA DE INTELIGÊNCIA POLICIAL
COORDENAÇÃO-GERAL DE INTELIGÊNCIA
Divisão de Contraineligência Policial

apreendida com GUSTAVO HENRIQUE e SUELEN a quantia de R\$ 99 mil reais em espécie, não tendo sido apresentados documentos que comprovariam sua origem lícita.

Conforme Informação nº 025/2019 – DICINT/CGI/DIP/PF (anexo 8 da medida cautelar nº 1017553-96.2019.4.01.3400), o RIF/COAF nº 43564/2019 apontou diversas transações financeiras suspeitas em nome de GUSTAVO HENRIQUE ELIAS SANTOS e sua companheira SUELEN PRISCILA DE OLIVEIRA. Pelo referido RIF/COAF, verifica-se que GUSTAVO HENRIQUE movimentou em sua conta no Banco Original (agência 0001, conta 7669429), entre os dias 18/04/2018 e 29/06/2018, o montante de R\$ 424.000,00, sendo que o mesmo informou em seu cadastro bancário possuir a renda mensal de R\$ 2.866,00 e exercer a atividade de empresário.

Conforme Relatório de Análise Bancária nº 01/2019/NO/DICINT/CGI/DIP/PF, SUELEN PRISCILA DE OLIVEIRA realizou operações financeiras, no período de 10/01/2018 a 18/10/2019, no Banco Original e Banco Itaú, que alcançaram o total bruto (sem expurgos) de R\$ 827.555,17 (créditos).

Por sua vez, de acordo como Laudo de Análise Contábil-Financeira nº 2161/2019-INC/DITEC/PF, SUELEN PRISCILA movimentou no período de 01/01/2019 a 17/07/2019, o valor bruto de R\$ 204.409,32, conforme tabela abaixo:

SUELEN PRISCILA DE OLIVEIRA (427.742.138-51)						
Ano	Créditos (R\$)			Débitos (R\$)		
	Brutos	Expurgos	Líquidos	Brutos	Expurgos	Líquidos
2019	204.409,32	100.797,32	103.612,00	103.955,57	100.000,00	3.955,57

GUSTAVO afirmou à Polícia Federal que utiliza o nome de SUELEN PRISCILA DE OLIVEIRA para movimentar seus recursos financeiros, mas que ela desconheceria suas atividades comerciais ou negócios que realizava. SUELEN PRISCILA também alegou desconhecer o envolvimento de GUSTAVO HENRIQUE ELIAS SANTOS com fraudes bancárias e outros golpes realizado pela internet, afirmando que seu companheiro






MJSP - POLÍCIA FEDERAL
DIRETORIA DE INTELIGÊNCIA POLICIAL
COORDENAÇÃO-GERAL DE INTELIGÊNCIA
Divisão de Contrainteligência Policial

possuiria como fonte de renda os pagamentos que recebe como DJ e os rendimentos conseguidos com a comercialização de criptomoedas.

Entretanto, foram encontradas informações nos aparelhos celulares apreendidos na residência do casal a evidenciar que SUELEN PRISCILA DE OLIVEIRA tem conhecimento e auxilia nas fraudes bancárias praticadas por GUSTAVO HENRIQUE ELIAS SANTOS. Segundo a Informação nº 027/2019-DICINT/CGI/DIP, foram encontrados diálogos no aplicativo WhatsApp entre GUSTAVO HENRIQUE, identificado como "Guto Amor" (11-972798093) e SUELEN, identificada como "Suélen Priscila" (11-973792405), onde GUSTAVO informa resultados de consultas de CPF e Suelen encaminha fotos de cartões de créditos de terceiros.

Também no e-mail djgutodubra@icloud.com foram encontradas algumas imagens que indicam provável falsificação de um comprovante em nome de SUELEN, que foi alterada para Kaio Alves Higor:



A relação criminosa entre WALTER DELGATTI NETO e GUSTAVO HENRIQUE ELIAS SANTOS foi inicialmente constatada pela instauração do IPL nº 38/2016, que tramitou na Delegacia da Polícia Federal em Araraquara/SP. No referido inquérito policial, WALTER DELGATTI NETO compareceu na Polícia Federal para relatar ter recebido de GUSTAVO HENRIQUE ELIAS SANTOS dinheiro falsificado, tendo apresentado uma cédula de R\$ 100 aparentemente falsa (Informação nº 023/19 – DICINT/CGI/DIP/PF).

0





MJSP - POLÍCIA FEDERAL
DIRETORIA DE INTELIGÊNCIA POLICIAL
COORDENAÇÃO-GERAL DE INTELIGÊNCIA
Divisão de Contraineligência Policial

Esta notícia-crime feita por WALTER DELGATTI NETO contra GUSTAVO HENRIQUE ELIAS SANTOS aparentemente seria apenas um pequeno desentendimento entre parceiros no crime. Em notícia publicada no em maio de 2013, foi informado que a Polícia Rodoviária da PM/SP havia apreendido estelionatários em um veículo, com placa de Araraquara/SP, no qual foram encontrados vários documentos e cartões de crédito de débito falsos, folhas de cheques e um extrato bancário falso constando na conta o valor de R\$ 1.834.111,83. Ainda segundo referida reportagem³, WALTER DELGATTI NETO foi recolhido ao Centro de Triagem e seus parceiros liberados, sendo que um deles foi identificado na matéria pelas iniciais GHES (GUSTAVO HENRIQUE ELIAS SANTOS).

Outros elementos de prova encontrados durante as investigações reforçam o envolvimento criminoso entre WALTER DELGATTI NETO e GUSTAVO HENRIQUE ELIAS SANTOS. Por exemplo, de acordo com a Informação nº 027/2019-DICINT/CGI/DIP, foram encontradas conversas em aplicativo (*iMessage*) entre GUSTAVO, identificado como "Guto Dubriss" (11-975770849) e WALTER DELGATTI NETO, identificado como "walterdelgattineto@icloud.com". Nos diálogos WALTER NETO descreve métodos de fraudes bancárias que pratica, usando coleta de códigos SMS usando uma "KL". No ambiente cibernético, "KL" se refere à abreviação de *Key Logger*, que indica ferramenta usada para registrar informações digitadas por vítimas com o intuito de obtenção de números de acesso de contas bancárias e senhas.

Do mesmo modo, WALTER NETO, após negociar a obtenção de "chip" (cartões SIM para smartphones) da empresa Claro por R\$ 400 reais, pergunta a GUSTAVO se um "Lara" (Laranja) que "rodou" (foi preso) do Banco do Brasil era do GUSTAVO, mencionando que o referido foi preso sacando R\$ 40.000,00 em Araraquara/SP. WALTER diz ainda que iria em uma agência do Itaú sacar dinheiro com um RG, ao que GUSTAVO responde para não falar este tipo de coisa por mensagem. Por fim há menção ao aplicativo *WICKR*, que é um conhecido aplicativo de mensagens criptografadas.

³ http://saocarlosnews.com/noticias_sub.php?id=920&fb=1





**MJSP - POLÍCIA FEDERAL
DIRETORIA DE INTELIGÊNCIA POLICIAL
COORDENAÇÃO-GERAL DE INTELIGÊNCIA
Divisão de Contrainteligência Policial**

Analisando o conteúdo do e-mail djgutodubra@icloud.com, utilizado por GUSTAVO HENRIQUE, foram ainda encontradas imagens relacionadas à falsificação de um documento de identidade em nome de Antônio Moreira Mendes, no qual colocada a foto de WALTER DELGATTI NETO:



Do mesmo modo, deve ser ressaltado que os dois arquivos de áudio que registraram WALTER DELGATTI NETO realizando técnicas de engenharia social visando acessar contas bancárias de duas vítimas, acima mencionados, foram enviados ao e-mail tadanado@icloud.com (WALTER) por GUSTAVO HENRIQUE ELIAS SANTOS, através do e-mail djgutodubra@hotmail.com:



Pode-se afirmar, também, que SUELEN PRISICILA teria conhecimento dos crimes praticados por WALTER DELGATTI NETO e seu parceiro GUSTAVO HENRIQUE ELIAS







MJSP - POLÍCIA FEDERAL
DIRETORIA DE INTELIGÊNCIA POLICIAL
COORDENAÇÃO-GERAL DE INTELIGÊNCIA
Divisão de Contraineligência Policial

SANTOS. O vínculo entre os três foi inicialmente identificado em razão de matéria jornalística que reportou a prisão de WALTER DELGATTI NETO na cidade de Penha/SC, ocorrida em maio de 2015, quando este tentou se passar por delegado da DEIC de São Paulo ao entrar em um parque de diversões, tendo sido apreendidos armas e munições em seu veículo. Segundo a reportagem⁴, WALTER DELGATTI NETO estava hospedado em um hotel, no centro de Itajaí/SC, juntamente com o casal GUSTAVO HENRIQUE ELIAS SANTOS e SUELEN PRISCILA DE OLIVEIRA, sendo estes encaminhados para a delegacia de Penha/SC e posteriormente liberados. No quarto de WALTER DELGATTI também foram encontrados 80 pacotes com 200 comprimidos que seriam anabolizantes.

O último integrante do "Grupo de Araraquara" seria DANILO CRISTIANO MARQUES, que atuaria como interposta pessoa de WALTER DELGATTI NETO, figura também conhecida no meio jurídico-policial como "testa-de-ferro", bem como na arregimentação de pessoas que pudessem emprestar seus nomes e contas bancárias para receber transferências de recursos obtidos nos golpes aplicados, conhecidos como "laranjas" ou "lara", atuando, assim, diretamente nos crimes.

DANILO CRISTIANO MARQUES relatou ter emprestado sua conta bancária no Banco do Brasil para WALTER DELGATTI NETO, que passou a ser utilizada exclusivamente por este para a realização de transferências e pagamentos diversos. Do mesmo modo, DANILO MARQUES confirmou ter comprado dólares americanos a pedido de WALTER DELGATTI NETO, transações estas ocorridas em casas de câmbio localizadas em São Paulo/SP, Rio de Janeiro/RJ e Natal/RN. Segundo afirmou DANILO MARQUES em suas declarações, WALTER DELGATTI NETO teria efetuado a compra de moeda estrangeira tendo em vista sua intenção de morar no exterior, sendo que ele não teria revelado qual seria a origem daqueles recursos.

Também de acordo com a Informação nº 076/2018 – DFIN/DICOR/PF (anexo 5 da medida cautelar nº 1017553-96.2019.4.01.3400), foram verificadas diversas operações

⁴ <https://diarinho.com.br/noticias-quentinhas/falso-delegado-e-presno-no-beto-carrero/>





MJSP - POLÍCIA FEDERAL
DIRETORIA DE INTELIGÊNCIA POLICIAL
COORDENAÇÃO-GERAL DE INTELIGÊNCIA
Divisão de Contraineligência Policial

financeiras suspeitas, ocorridas entre 01/12/2016 e 05/12/2016, efetivadas por WALTER DELGATTI NETO e DANILO CRISTIANO MARQUES, dentre outras pessoas, relacionadas à compra de dólares americanos e euros em lojas de câmbio situadas em aeroportos.

A comunicação do COAF anotou que as operações suspeitas de câmbio tinham o montante associado de R\$ 90.712,00 e que além das operações realizadas, outras operações de câmbio foram tentadas pelos envolvidos, mas frustradas em razão de terem sido consideradas suspeitas. As operações realizadas de câmbio ocorreram nos aeroportos de Internacional de Natal/RN e no Aeroporto Internacional do Rio de Janeiro.

DANILO CRISTIANO MARQUES confirmou ter comprado dólares americanos a pedido de WALTER DELGATTI NETO, transações estas ocorridas em casas de câmbio localizadas em São Paulo/SP, Rio de Janeiro/RJ e Natal/RN. Segundo afirmou DANILO MARQUES em suas declarações, WALTER DELGATTI NETO teria efetuado a compra de moeda estrangeira tendo em vista sua intenção de morar no exterior, sendo que ele não teria revelado qual seria a origem daqueles recursos.

A atuação de DANILO CRISTIANO como interporsta pessoa de WALTER DELGATTI poder ser demonstra pelas informações constantes no Laudo de Perícia Criminal Contábil-Financeiro nº 2161/2019-INC/DITEC/PF. Foi verificado que, no ano de 2018, DANILO CRINSTIANO transferiu o total de R\$ 172.682,50 para a empresa AME RESTAURANTE LTDA, de propriedade de THIAGO ELIEZER, em uma evidente triangulação de recuros que seriam de WALTE DELGATTI NETO.

Também foi realizada a análise do conteúdo extraído do aparelho celular Apple iPhone 8 Plus (A1897), apreendido em posse de DANILO CRISTIANO MARQUES, materializado no RAMA nº 12/2109 DICINT/CGI/DIP/PF. Após análise dos dados extraídos do aparelho em questão pela equipe de policiais federais do Instituto Nacional de Criminalística, foi verificada a presença de conversas nos aplicativos WhatsApp e Telegram que confirmam vínculos entre DANILO CRISTIANO MARQUES e WALTER DELGATTI NETO, sendo que este

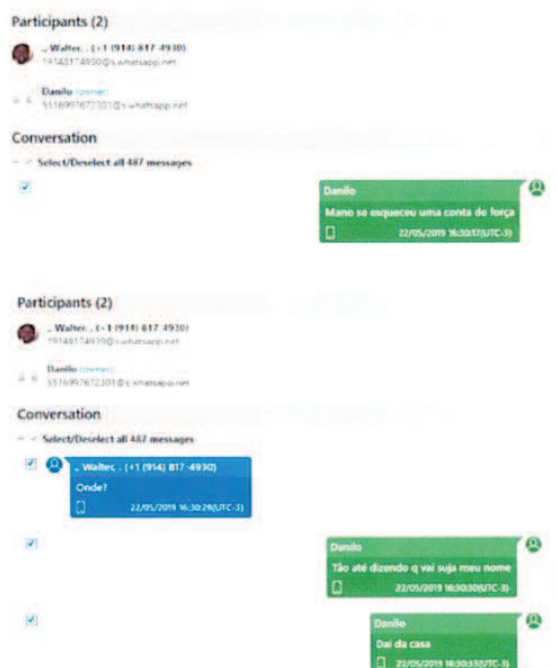




MJSP - POLÍCIA FEDERAL
DIRETORIA DE INTELIGÊNCIA POLICIAL
COORDENAÇÃO-GERAL DE INTELIGÊNCIA
Divisão de Contrainteligência Policial

último se comunicava com DANILO CRISTIANO MARQUES a partir de três números distintos:
+1 914 8174930; +1 914 4616976; +55 16 997888653.

Nos diálogos pelo aplicativo WhatsApp, pode-se apreender que DANILO MARQUES cedeu a WALTER DELGATTI NETO seu nome para que este formalizasse o contrato de aluguel de um imóvel, bem como para formalizar cadastro de consumidor na CPFL (Companhia Paulista de Força e Luz) e na empresa NET, provedora de internet. Conforme trechos abaixo, no dia 22 de maio de 2019 DANILO cobra WALTER sobre uma conta de luz em atraso:



No dia 27 de maio de 2019, WALTER informa a DANILO que já efetuou o pagamento da luz, NET e condomínio:

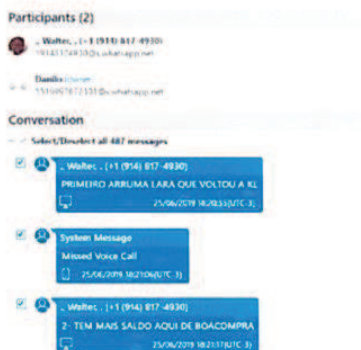




MJSP - POLÍCIA FEDERAL
DIRETORIA DE INTELIGÊNCIA POLICIAL
COORDENAÇÃO-GERAL DE INTELIGÊNCIA
Divisão de Contrainteligência Policial



Por meio das mensagens do WhatsApp, pode-se concluir que DANILO MARQUES era parceiro de WALTER NETO nas empreitadas criminosas envolvendo fraudes bancárias. DANILO tinha a função de encontrar "laranjas" para WALTER NETO depositar o dinheiro sabidamente oriundo das fraudes, situação que rendia a DANILO valores entre 20% e 50% de cada transferência. Conforme trecho abaixo do diálogo ocorrido em 25 de junho de 2019, WALTER se refere a "laranjas" como "lara":



Nesta ocasião a preocupação de WALTER era que o dinheiro retornasse rapidamente, afirmando ter disponível 15k (R\$ 15.000,00):





MJSP - POLÍCIA FEDERAL
DIRETORIA DE INTELIGÊNCIA POLICIAL
COORDENAÇÃO-GERAL DE INTELIGÊNCIA
Divisão de Contrainteligência Policial

Participants (2)

Walter, . (+1 (914) 817-4930)
19143174930@whatsapp.net

Danilo (owner)
5516997672301@whatsapp.net

Conversation

Select/Deselect all 487 messages

Walter, . (+1 (914) 817-4930)
ACHA QUE CONSEGUIE DINHEIRO IMEDIATO?
25/06/2019 18:21:33(UTC-3)

Walter, . (+1 (914) 817-4930)
TEM 15K
25/06/2019 18:21:34(UTC-3)

Danilo
Manda
25/06/2019 18:21:29(UTC-3)

WALTER NETO então afirma que teria combinado com CRASH (THIAGO ELIEZER MARTINS SANTOS) sobre aumentar a comissão de DANILO de 20% para 50%:

Participants (2)

Walter, . (+1 (914) 817-4930)
19143174930@whatsapp.net

Danilo (owner)
5516997672301@whatsapp.net

Conversation

Select/Deselect all 487 messages

Walter, . (+1 (914) 817-4930)
FALEI COM O CRASH
25/06/2019 18:21:32(UTC-3)

Walter, . (+1 (914) 817-4930)
ELE DISSE OS SEGUINTE
25/06/2019 18:21:38(UTC-3)

Walter, . (+1 (914) 817-4930)
VOCE ESTAVA GANHANDO 20%
25/06/2019 18:21:42(UTC-3)





MJSP - POLÍCIA FEDERAL
DIRETORIA DE INTELIGÊNCIA POLICIAL
COORDENAÇÃO-GERAL DE INTELIGÊNCIA
Divisão de Contraineligência Policial

Participants (2)

Walter, (+1 (914) 817-4930)
19148174930@s.whatsapp.net

Daniilo (owner)
5519997672301@s.whatsapp.net

Conversation

Select/Deselect all 487 messages

- ✓ Walter, (+1 (914) 817-4930)
A GENTE TE DA 50%
25/06/2019 18:21:46(UTC-3)
- ✓ Walter, (+1 (914) 817-4930)
OU SEJA
25/06/2019 18:21:47(UTC-3)
- ✓ Walter, (+1 (914) 817-4930)
DE 15K
25/06/2019 18:21:50(UTC-3)

Depreende-se do diálogo acima que CRASH ocupava posição de decisão na empreitada criminosa, visto que WALTER o consultou antes de cientificar DANILO sobre esta decisão. Há outros trechos de diálogos em que DANILO recebe mensagens de WALTER com referências a CRASH.

Nos diálogos abaixo, fica evidente que WALTER aplica uma fraude bancária e tenta realizar a transferência para a conta de "laranja", indicado por DANILO, porém a transferência foi bloqueada por suspeita de fraude, conforme o código "ERRO 408" do banco ITAU. Entretanto, a sequência dos diálogos torna inteligível o desenrolar da empreitada, tendo WALTER perguntado a DANILO se ele possui "laranja" do banco ITAU em funcionamento, DANILO responde que sim (imagem abaixo):





MJSP - POLÍCIA FEDERAL
DIRETORIA DE INTELIGÊNCIA POLICIAL
COORDENAÇÃO-GERAL DE INTELIGÊNCIA
Divisão de Contrainteligência Policial



WALTER NETO então informa que tem R\$ 3.858,00 para enviar, quando então DANILO repassa imediatamente o número de conta corrente e agência através da foto de um cartão magnético de um terceiro para que WALTER realize a transferência do valor:



Cerca de 7 minutos após, WALTER pergunta a DANILO se é possível ver o saldo:

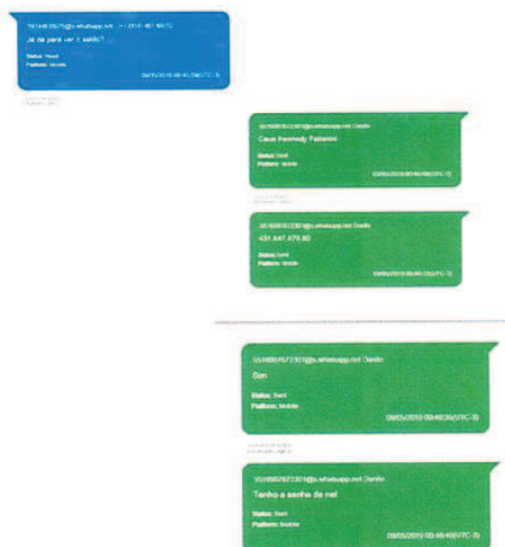




MJSP - POLÍCIA FEDERAL
DIRETORIA DE INTELIGÊNCIA POLICIAL
COORDENAÇÃO-GERAL DE INTELIGÊNCIA
Divisão de Contraineligência Policial



DANILO prontamente responde a WALTER que sim, pois possui a senha de internet *banking* da conta enviada anteriormente, o que fornece indícios de que o suposto "laranja" é uma pessoa com participação na fraude, que fornece seus dados bancários e dados de acesso ao sistema internet *banking* para o recebimento do dinheiro e transferência imediata para outras contas, evitando assim o bloqueio dos valores:





MJSP - POLÍCIA FEDERAL
DIRETORIA DE INTELIGÊNCIA POLICIAL
COORDENAÇÃO-GERAL DE INTELIGÊNCIA
Divisão de Contrainteligência Policial

WALTER DELGATTI envia mensagem a DANILO informando que a suposta vítima da fraude possui "12 de cartão", provavelmente R\$ 12.000,00 disponíveis para uso em cartão de crédito. WALTER informa ainda que "dá pra puxar" este valor, o que DANILO congratula-se enviado a WALTER o texto "Toppo":



Por volta de 01h00 da manhã, WALTER continua insistindo com DANILO para saber se o dinheiro caiu na conta destinatária, porém DANILO somente responde às 07h00 da manhã:



DANILO então lamenta a WALTER, informando que ocorreu o erro 408, referindo-se ao código do Banco Itaú referente a bloqueio causado por suspeita de fraude:

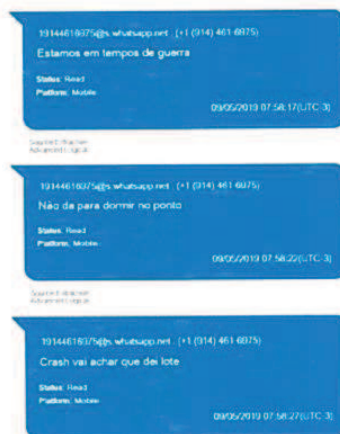




MJSP - POLÍCIA FEDERAL
DIRETORIA DE INTELIGÊNCIA POLICIAL
COORDENAÇÃO-GERAL DE INTELIGÊNCIA
Divisão de Contrainteligência Policial



Neste momento em que lamentam a falha na empreitada criminosa, WALTER faz novamente faz referência a CRASH, dizendo que "Crash vai achar que dei lote" (calote), ou seja, CRASH iria achar que foi passado para trás, deixando claro que este último teve papel preponderante na realização da empreitada, possuindo direito sobre valor adquirido através da fraude:



WALTER continua o diálogo afirmando que às 6h da manhã CRASH já havia enviado mensagem mandando sacar logo o dinheiro, o que mais uma vez confirma a preponderância de CRASH sobre os dois, quando então DANILO responde a WALTER que "este





MJSP - POLÍCIA FEDERAL
DIRETORIA DE INTELIGÊNCIA POLICIAL
COORDENAÇÃO-GERAL DE INTELIGÊNCIA
Divisão de Contrainteligência Policial

foi isolado", dando certeza da habitualidade e sucesso frequente em outras situações de mesmo tipo:



Na sequência WALTER diz para tentarem mais tarde e que "tinha 30K" (R\$ 30.000) e que param "27 de boleto" (R\$ 27.000). Estas mensagens formam a convicção da frequência nas fraudes e sugerem que parte do dinheiro poderia retornar aos fraudadores por meio de boletos que simulariam pagamentos a pessoas ou empresas por serviços realizados:

Q





MJSP - POLÍCIA FEDERAL
DIRETORIA DE INTELIGÊNCIA POLICIAL
COORDENAÇÃO-GERAL DE INTELIGÊNCIA
Divisão de Contraineligência Policial



Também foram extraídas mensagens entre WALTER NETO e DANILO CRISTIANO pelo aplicativo Telegram. Em diálogo de 17/07/2019, por meio do Telegram, WALTER pede a DANILO que envie dados de "laranja" para "valor alto", conforme diálogo abaixo:





MJSP - POLÍCIA FEDERAL
DIRETORIA DE INTELIGÊNCIA POLICIAL
COORDENAÇÃO-GERAL DE INTELIGÊNCIA
Divisão de Contraineligência Policial

DANILO MARQUES, após 4 minutos, responde informando dados bancários, incluindo senha de internet banking, de três pessoas diferentes, ressaltando-se que DANILO utilizava do nome de usuário QUEIROZ no Telegram (id 739990517) enquanto WALTER utilizava o id 753621143:

Quantal 739990517
BANCO DO BRASIL 001
thana bianca ribeiro cunha
AGENCIA 01676
CONTA 454806
SENHA DA NET 85010676
CPF 09462705623

Banco do Brasil
Flavio Jeronimo dos Santos nascimento
Agência 16545
Conta 57949.2
Senha da net 21103922
CPF 39231903570

Banco do Brasil
Elisangela Cristina de Oliveira Silva
Agência 65129
Conta 166073
Senha net 15022008
CPF 22414219674

13.37.34-0300

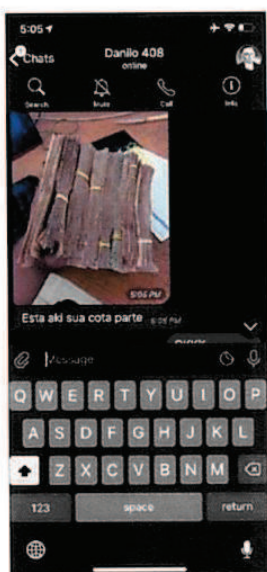
Por sua vez, também foram identificados elementos que evidenciariam o relacionamento criminoso entre DANILO CRISTIANO e GUSTAVO HENRIQUE ELIAS SANTOS. Em declarações prestadas à Polícia Federal (fls. 86/88), DANILO CRISTIANO MARQUES afirmou que utilizava o codinome "CHACAL", tendo sido encontrada no arquivo de nuvem da conta gutodubra@icloud.com a seguinte mensagem entre GUSTAVO HENRIQUE ELIAS e um interlocutor identificado como "Hhh Chacal", podendo se tratar de DANILO, referente a saques bancários:





MJSP - POLÍCIA FEDERAL
DIRETORIA DE INTELIGÊNCIA POLICIAL
COORDENAÇÃO-GERAL DE INTELIGÊNCIA
Divisão de Contrainteligência Policial

Também foi encontrada no e-mail gutodubra@icloud.com a troca de mensagens entre GUTO e "DANILO 408", com imagem de cédulas amarradas e a frase "Esta aki sua cota parte":



Do mesmo modo, nos arquivos vinculados ao e-mail gutodubra@icloud.com, utilizado por GUSTAVO HENRIQUE ELIAS, foram encontradas imagens de comprovantes de depósito, no valor de R\$ 1 mil cada, realizados em 2018 na conta de DANILO CRISTIANO MARQUES:





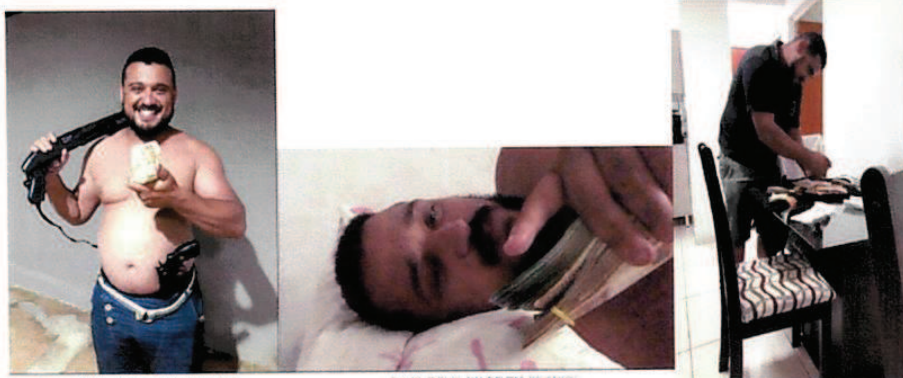
MJSP - POLÍCIA FEDERAL
DIRETORIA DE INTELIGÊNCIA POLICIAL
COORDENAÇÃO-GERAL DE INTELIGÊNCIA
Divisão de Contrainteligência Policial

Ressalte-se que as instituições financeiras ainda não fizeram a transmissão completa dos dados bancários dos investigados referentes ao ano de 2018, não sendo possível confirmar a origem ou efetividade dos depósitos acima. Entretanto, em análise preliminar formalizada no Relatório de Análise Bancária nº 01/2019/NO/DICINT/CGI/DIP/PF, foi informado que DANILO CRISTIANO MARQUES movimentou em contas nos Bancos Inter S/A e Banco do Brasil, no período entre 20/08/2018 a 26/12/2018, o montante a crédito de R\$ 893.092,43 (sem expurgos).

Por sua vez, de acordo como Laudo de Análise Contábil-Financeira nº 2161/2019-INC/DITEC/PF, DANILO CRISTIANO MARQUES movimentou no período de 01/01/2019 a 17/07/2019, o valor bruto de R\$ 75.129,25 conforme tabela abaixo:

DANILO CRISTIANO MARQUES (370.074.428-54)					
Ano	Créditos [R\$]			Débitos [R\$]	
	Brutos	Expurgos	Líquidos	Brutos	Líquidos
2019	75.129,25	11.928,06	63.201,19	75.208,41	11.928,06
					63.280,35

Por fim, de acordo com a Informação nº 55/2019-DICINT/CGI/DIP/PF, foram encontradas imagens que retratam DANILO CRISTIANO MARQUES ostentando quantidade imprecisa de dinheiro em espécie, bem como arma de fogo ou simulacro:





MJSP - POLÍCIA FEDERAL
DIRETORIA DE INTELIGÊNCIA POLICIAL
COORDENAÇÃO-GERAL DE INTELIGÊNCIA
Divisão de Contrainteligência Policial

9.1.2 – THIAGO ELIEZER MARTINS SANTOS

THIAGO ELIEZER MARTINS SANTOS, que também é conhecido pelo apelido "CHICLETE", somente foi identificado após a primeira fase ostensiva da Operação Spoofing, o que permitiu que ele pudesse interferir na instrução criminal destruindo as provas da prática de crimes que estavam em seu poder. Nas declarações de fls. 495/499, THIAGO ELIEZER confirmou à Polícia Federal que, após a prisão de WALTER DELGATTI NETO, apagou de seus celulares e demais dispositivos eletrônicos todas as mensagens, arquivos e aplicativos, tendo também deletado o *software* da BRVOZ que estava instalado em seu computador.

Entretanto, com base em diversas evidências colhidas na primeira fase da Operação Spoofing, foi possível comprovar que integrantes do "Grupo de Araraquara" se relacionavam com THIAGO ELIEZER MARTINS SANTOS, pessoa conhecida no submundo dos crimes cibernéticos pelo codinome "CRASH" ou "CRASH OVERWING⁵" (citado erroneamente por WALTER DELGATTI NETO como "CRASH OVERLONG").

À Polícia Federal THIAGO ELIEZER negou ou permaneceu em silêncio quando foi questionado se de fato utilizava o codinome "CRASH", fato comprovado, entretanto, por diversas evidências obtidas durante às investigações. Conforme Informação nº 44/2019, foi encontrado no fórum GUJ, utilizado por profissionais do ramo de tecnologia, o perfil "Crash_Overwing" vinculado ao nome "Chicleteh", alcunha assumida por THIAGO ELIEZER, corroborando a associações entre o codinome CRASH OVERWING e o investigado THIAGO ELIEZER:



⁵ Crash Override é o nome do personagem principal do filme Hackers, filmado em 1995, no qual foram refletidos os ideais estabelecidos no Manifesto Hacker, que é citado no filme.

