Sobre a rastreabilidade do envio de mídias na plataforma Whatsapp para o combate de crimes digitais

Miguel Freitas
miguel@cpti.cetuc.puc-rio.br
Engenheiro Eletrônico, Mestre em Telecomunicações, Doutor em Eletromagnetismo Aplicado, Pesquisador do Centro de Estudos em Telecomunicações (CETUC) – PUC-Rio

Organização geral da apresentação

1. Apresentação técnica demonstrando a viabilidade do rastreamento da origem das mídias enviadas através da plataforma Whatsapp e um possível descumprimento da legislação vigente (Lei do Marco Civil) por parte da empresa.

2. Aplicação da técnica ao caso das “fake news” na eleição de 2018 com a análise da propagação de mensagens em grupos de discussão política.

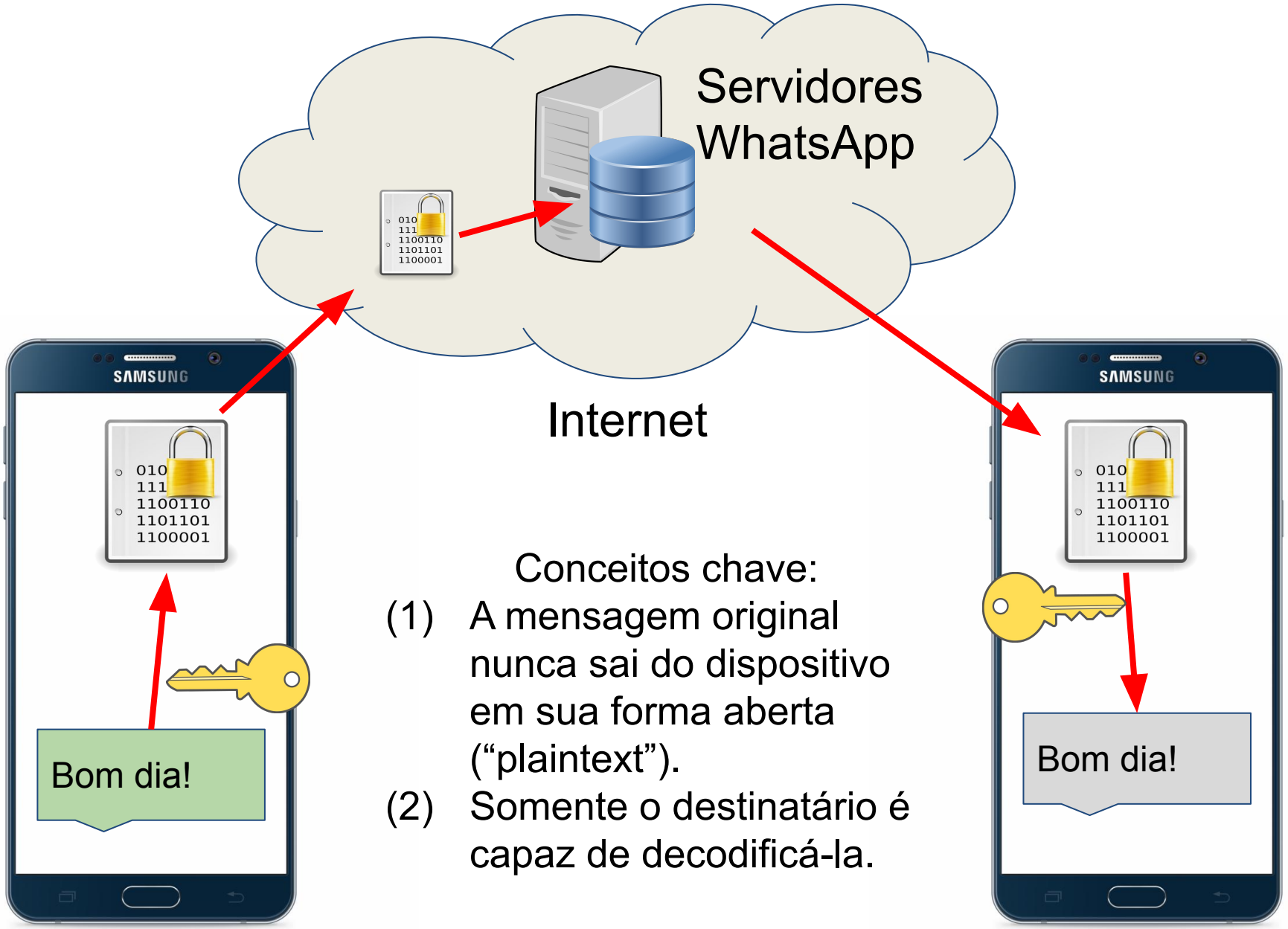
Sumário executivo 1/2

- Seria **tecnicamente** possível obter, com colaboração do WhatsApp, informações sobre a origem de uma mídia digital (imagem/vídeo/etc) enviada ou encaminhada através da plataforma.
- O encaminhamento entre grupos e usuários preserva a capacidade de rastreamento das mídias.
- A resposta do WhatsApp (23/01/2019) de que não preserva os registros de “upload” de mídia constitui uma possível violação do artigo 15 do Marco Civil. Há decisão de 2ª instância reconhecendo este descumprimento.
- O MPF foi provocado sobre esta questão (referência **PR-SP-00044139/2019**).

Sumário executivo 2/2

- A metodologia de identificação de mídias de WhatsApp foi aplicada em mensagens que circularam em 277 grupos de política durante as eleições.
- Foram analisados detalhadamente 16 casos de mídias com conteúdo falso (“fake news”) por critérios de relevância e de melhor rastreabilidade.
- Um relatório com os identificadores digitais (URLs) destes 16 casos, que poderiam ser usados para elaboração de solicitações judiciais, foi encaminhada à PGR em 26/11/2018 como uma contribuição pessoal e cidadã ao processo de investigação das “fake news”.

Criptografia fim-a-fim

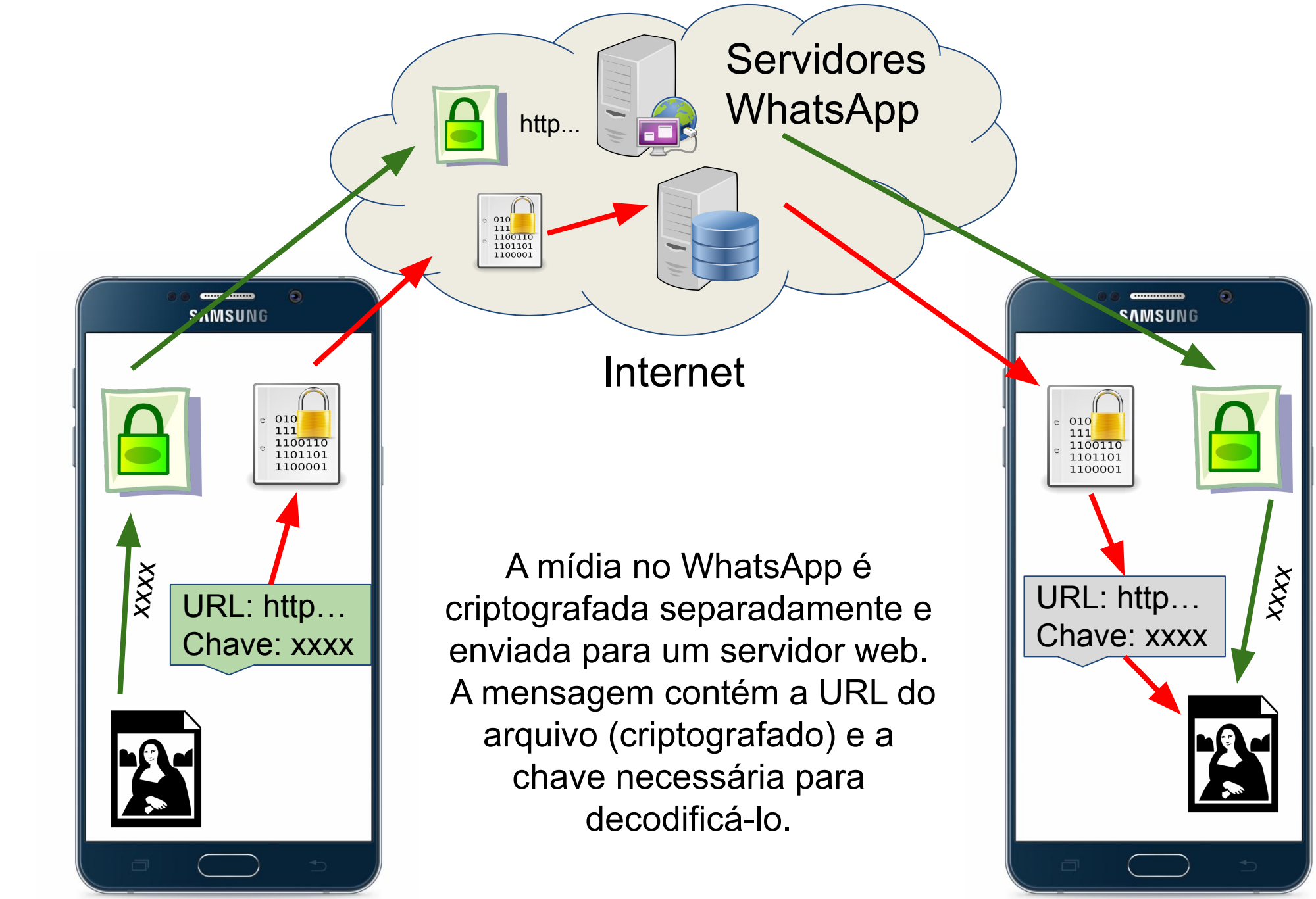


Conceitos chave:

(1) A mensagem original nunca sai do dispositivo em sua forma aberta (“plaintext”).

(2) Somente o destinatário é capaz de decodificá-la.

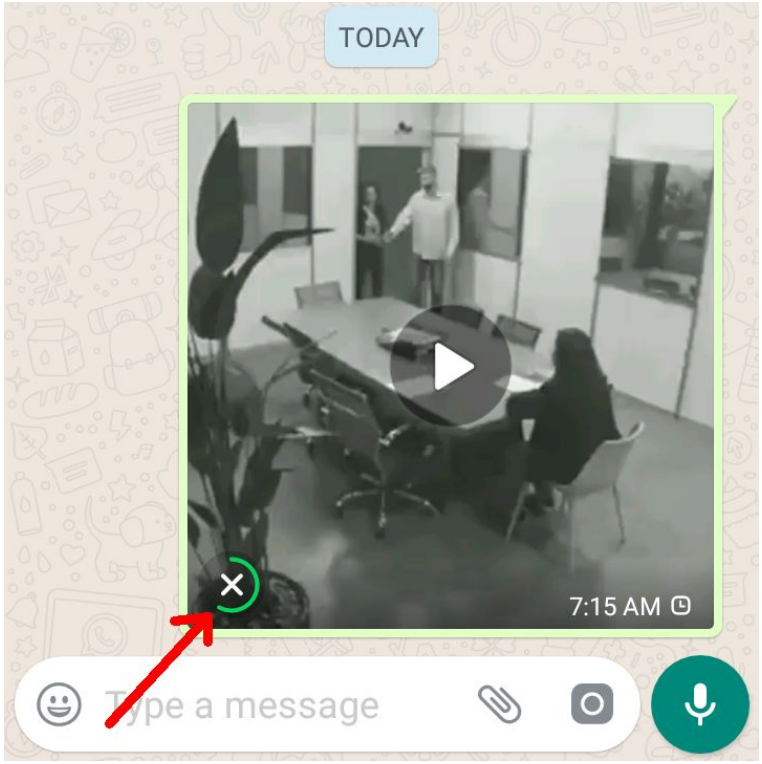
Envio de mídias com criptografia

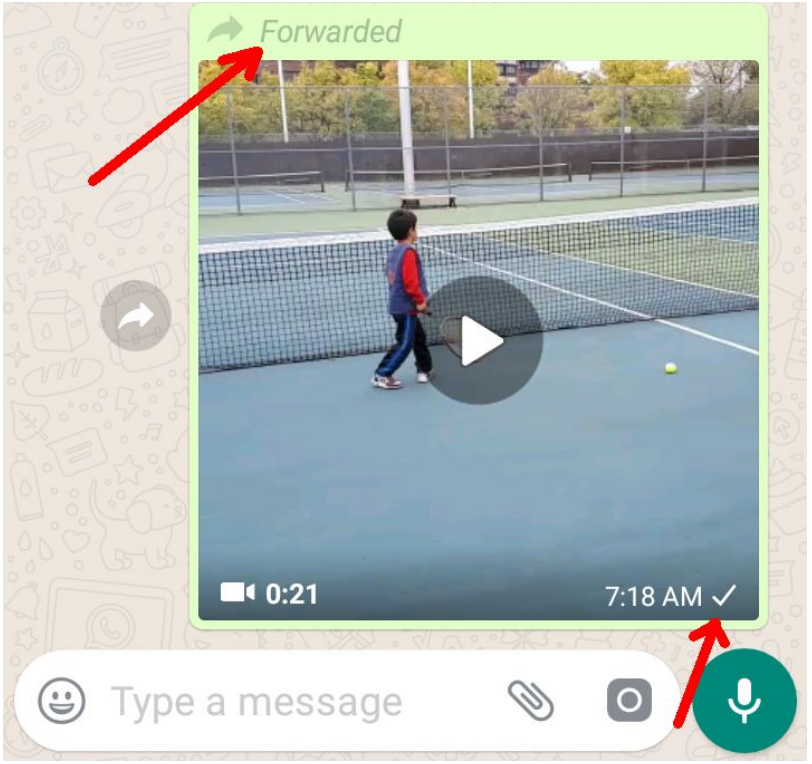


A mídia no WhatsApp é criptografada separadamente e enviada para um servidor web. A mensagem contém a URL do arquivo (criptografado) e a chave necessária para decodificá-lo.

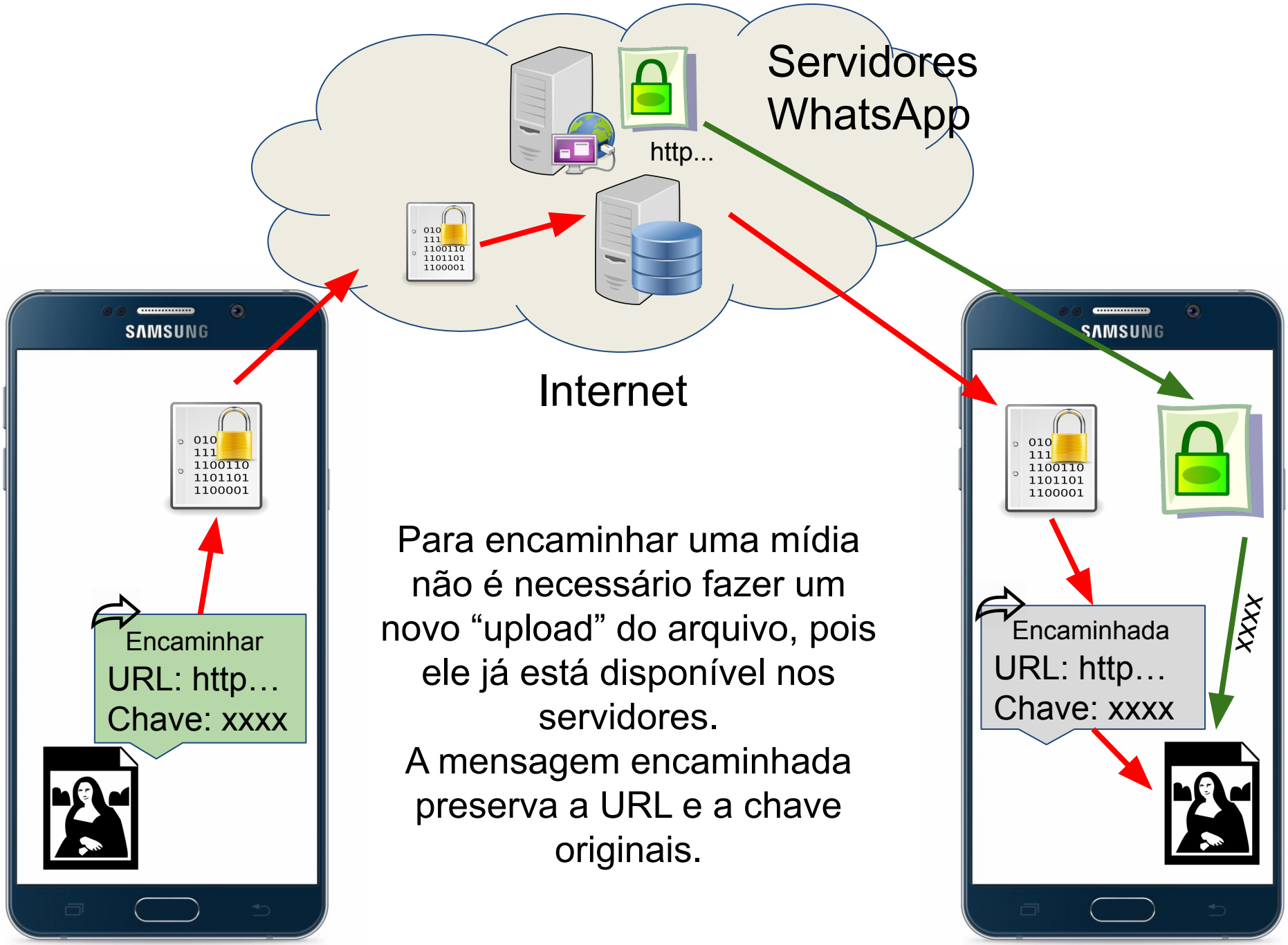
Envio de mídia original x encaminhamento

- O envio de uma mídia original implica no “upload” do arquivo (criptografado). O WhatsApp exibe indicador de progresso.
- Já o encaminhamento é instantâneo. Geralmente não há indicador de progresso e o “tick” (enviado) aparece imediatamente.



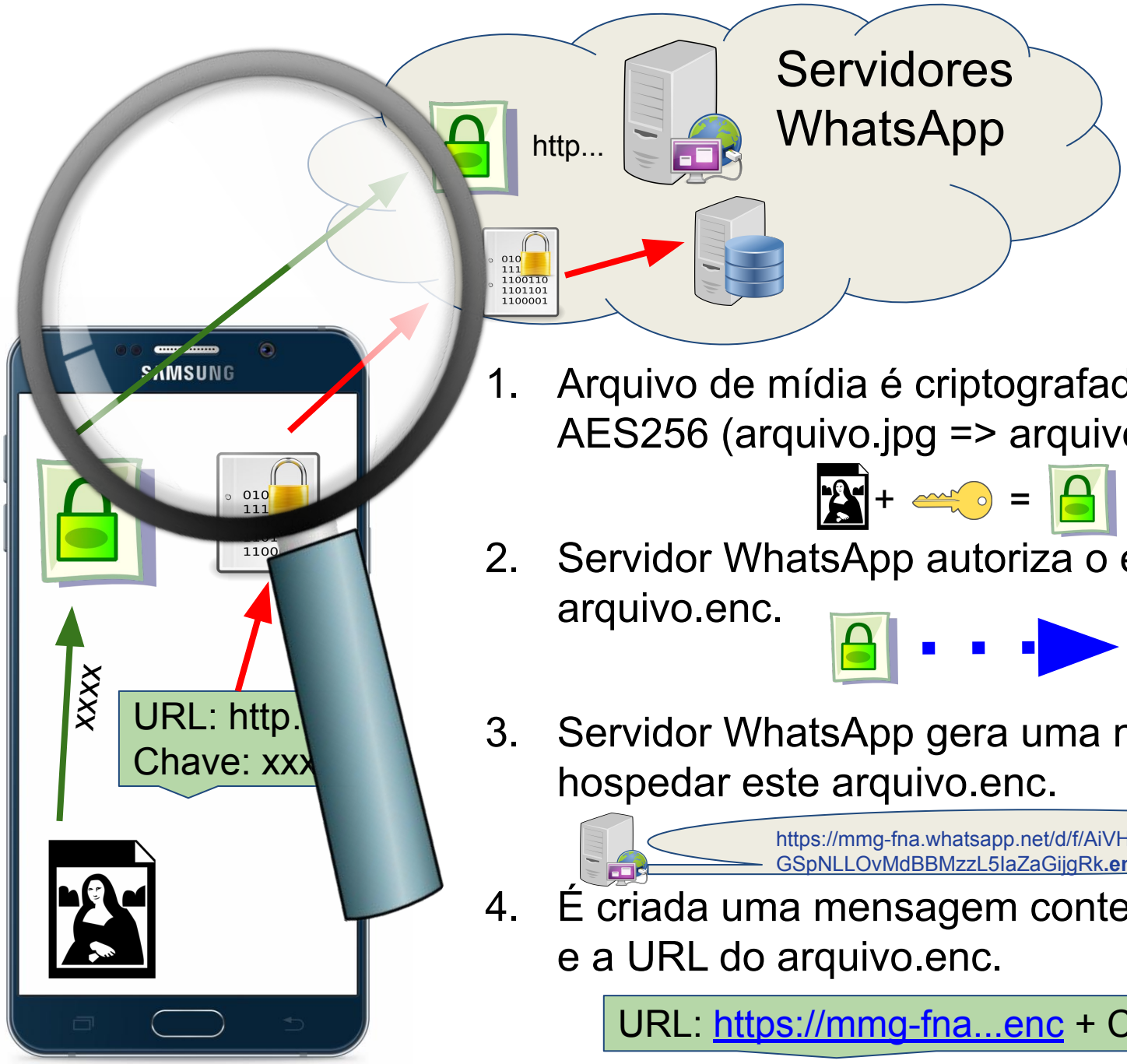


Encaminhamento de mídias



Para encaminhar uma mídia não é necessário fazer um novo “upload” do arquivo, pois ele já está disponível nos servidores.
A mensagem encaminhada preserva a URL e a chave originais.

Detalhes sobre o upload da mídia no WhatsApp



1. Arquivo de mídia é criptografado com chave AES256 (arquivo.jpg => arquivo.enc)

2. Servidor WhatsApp autoriza o envio (upload) do arquivo.enc.

3. Servidor WhatsApp gera uma nova URL para hospedar este arquivo.enc.

4. É criada uma mensagem contendo a chave AES256 e a URL do arquivo.enc.

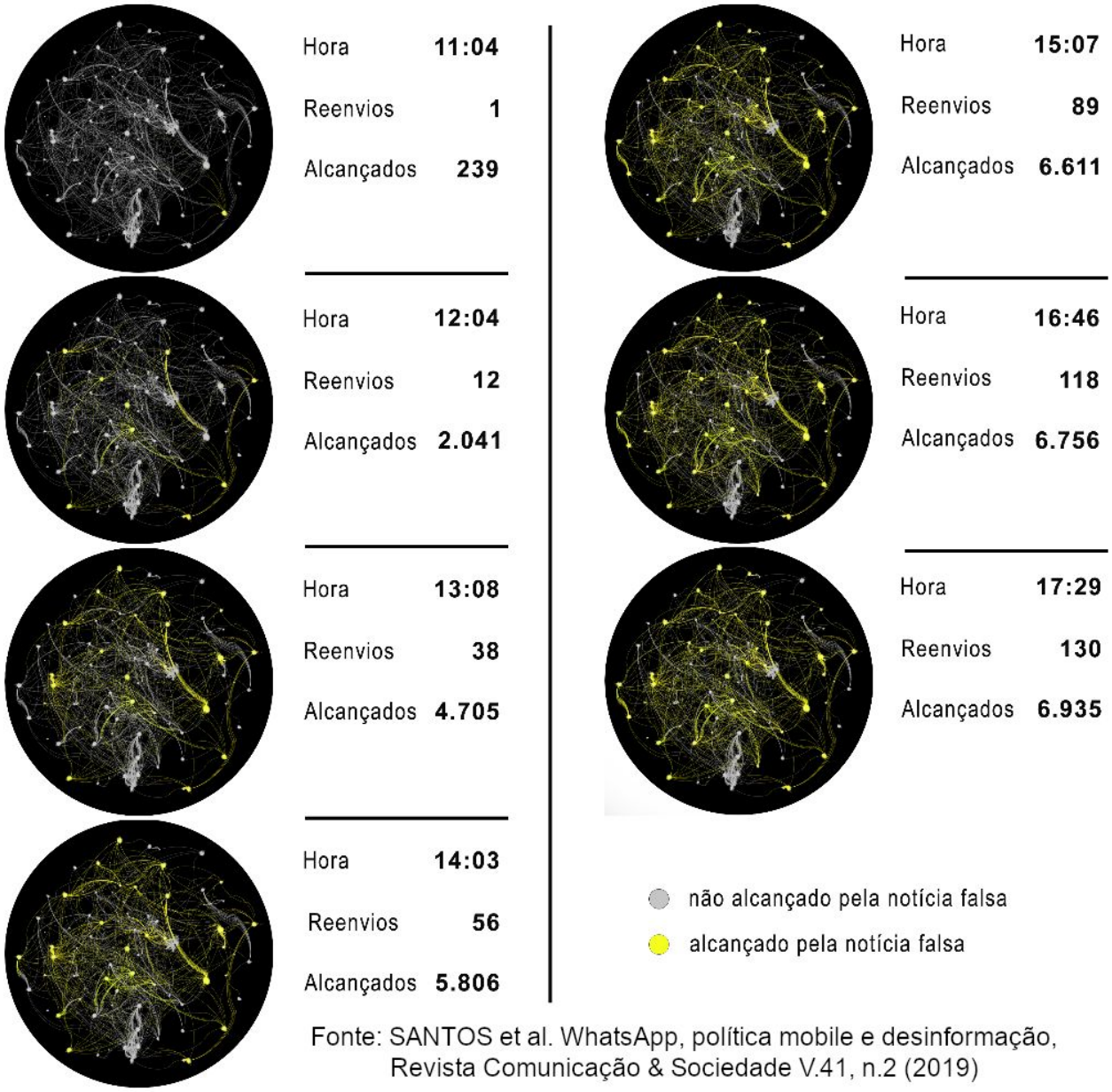
URL: https://mmg-fna...enc + Chave: xxxx

Provedores de aplicações de Internet

Aplicação	Hospedagem de sites Google, Facebook etc	WhatsApp
Autenticação	Exige autenticação do usuário para upload de arquivos	Exige autenticação do usuário para upload de arquivos
Endereço IP	Conhece o endereço IP do terminal que está fazendo upload	Conhece o endereço IP do terminal que está fazendo upload
URL	Gera URL que pode ser usado como identificador inequívoco nos termos da Lei 12.965/14 Art. 19 Par. 10	Gera URL que pode ser usado como identificador inequívoco nos termos da Lei 12.965/14 Art. 19 Par. 10
Guarda de registros de acesso	**É obrigado a manter os registros de acesso por 6 meses nos termos da Lei 12.965/14 Art. 15**	**?**

Propagação de mensagens em grupos

Notícia Falsa sobre o Tribunal Superior Eleitoral viralizando



Fonte: SANTOS et al. WhatsApp, política mobile e desinformação, Revista Comunicação & Sociedade V.41, n.2 (2019)

- Os usuários fazem os repasses entre grupos, produzindo a “viralização”.
- Muitos grupos de política possuem convites públicos.
- Por amostragem é possível estudar a dinâmica de propagação das mensagens.

Metodologia aplicada às eleições de 2018

- Analisados 277 grupos de política no período eleitoral e pré-eleitoral com convites públicos (todos os candidatos).
- Base com 799 mil mensagens, 15 mil participantes e 120 mil imagens compartilhadas.

Identificador do Grupo	Criado por	Em	Nome
13155376323-1539911183@g.us	13155376323	18-Oct-2018	Presidente Bolsonaro
14322174763-1539962947@g.us	14322174763	19-Oct-2018	
15852133699-1535336973@g.us	15852133699	26-Aug-2018	Bolsonaro2019
19017083924-1538707850@g.us	19017083924	04-Oct-2018	#EleNão ☭
5511948447729-1539054654@g.us	5511948447729	09-Oct-2018	OPERAÇÃO LAVA JATO
5511958225360-1469307515@g.us	5511958225360	23-Jul-2016	Contra a Mordaça
5511958391963-1539425135@g.us	5511958391963	13-Oct-2018	SOCIALISMO x CAPITALISMO
5511958755944-1528849627@g.us	5511958755944	12-Jun-2018	
5511958755944-1531605338@g.us	5511958755944	14-Jul-2018	
5511959756142-1521224993@g.us	5511959756142	16-Mar-2018	MovimentoSocialDemocracia
5511972315345-1497792293@g.us	5511972315345	18-Jun-2017	Política Brasil
5511972315345-1534876222@g.us	5511972315345	21-Aug-2018	#ChamaOMeirelles
5511972315345-1539777756@g.us	5511972315345	17-Oct-2018	

Seleção das mensagens analisadas

- Critério 1 - seleção de “fake news” feita pelo jornal “El País” em “Os whatsapps de uma campanha envenenada”
- Critério 2 - mídias (imagens) mais compartilhadas e comprovadamente falsas
- Critério 3 - mídias falsas com melhores características de rastreamento (URL preservada entre encaminhamentos)


28 OUT 2018 - 06:35 BRST

ESP | AME | BRA | CAT | ENG

EL PAÍS

eleições2018

NOTÍCIAS CANDIDATOS ANÁLISE PRIMEIRO VOTO PESQUISAS BRASIL DESIGUAL NO TWITTER WHATSAPPS CHAVES

Os 'whatsapps' de uma campanha envenenada

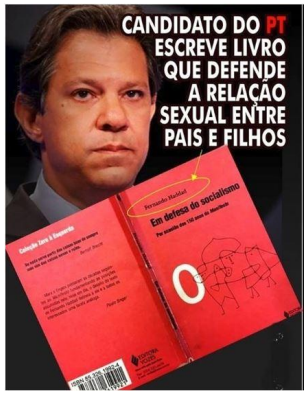
As eleições presidenciais levaram a campanhas agressivas de desinformação voltadas diretamente aos celulares dos eleitores. Em um país onde o uso do WhatsApp é enorme, mensagens carregadas de mentiras se tornaram virais. EL PAÍS entra em um grupo fictício para explicar o fenômeno. Os memes são reais.

Mensagens de mídia mais compartilhadas / rastreáveis (fake news em vermelho)

roup	alias	mediaHash	mediaUrl
182	enviar-20-aviao-haddad	jM79bumFtYq/0uJJB	https://mmg-fna.whatsap
129	cheque-68-milhoes-para-haddad	HsnsGACgquWOkD	https://mmg-fna.whatsap
115	Video-assaltos-armados-haddad-desencarceramento	gJuAG551Jhqk671a	https://mmg-fna.whatsap
98	Lula-decreto-sem-ler-ives-gandra	dsEynCorybYq8iAp	https://mmg-fna.whatsap
94	Zap-gabrielli-combina-bomba-folha-fakenews	S0TWnOEIFZTLkKo	https://mmg-fna.whatsap
95	Serie-bndes-inicio	30WDh8tV1RBXTL9	https://mmg-fna.whatsap
88	Urna-eletronica-cacamba-apreendida-Autazes1	E9rPfE1eyf+TPeXla	https://mmg-fna.whatsap
85	Bolsonaro-meddle-tropa-de-elite	JiA5pAfZ2F+Nrb/V/q	https://mmg-fna.whatsap
91	serie-bndes-200mi-bolivia	z5Nd912D+KRV/mN	https://mmg-fna.whatsap
103	Serie-bndes-agua-peru-racionamento-vitoria	ExUnwnBK+vwDx3q	https://mmg-fna.whatsap
84	vem-pra-rua-copa	v1SKhDp/2g0dVvcA	https://mmg-fna.whatsap
92	Serie-bndes-nicaragua-zero-empregos-brasil	PssMKvv6xRRqh89k	https://mmg-fna.whatsap
91	Haddad-jn-legenda-candidato-da-quadrilha-so-bonner	qz4rVRS3laX0HqGts	https://mmg-fna.whatsap
99	serie-bndes-8bi-argentina-nunca-mais-vamos-ver	Tt1toLCwMF53Kftrc	https://mmg-fna.whatsap
88	serie-bndes-1bi-panama	Qo+BmMXPRUo/PT	https://mmg-fna.whatsap
89	serie-bndes-300mi-benesse-montevideo	pW1avAftlA2sD1VnU	https://mmg-fna.whatsap
89	serie-bndes-11bi-venezuela	0iuA+KQ8hSmW0iKh	https://mmg-fna.whatsap
88	serie-bndes-180mi-chaco	PJN9jl6uq/UElPo6tm	https://mmg-fna.whatsap
90	Serie-bndes-ponte-orinoco	NsN8CavmvGKDn1l	https://mmg-fna.whatsap
90	Carreata-vitoria-bolsonaro-imperatriz	/ZIPqc+L0dnVVJGnj	https://mmg-fna.whatsap

Seleção de “fake news” do El Pais

- Nem todas as mensagens selecionadas possuem boa “rastreabilidade”.
- Mídias com diferentes versões (resolução/tamanho de arquivo) ou diferentes URLs podem indicar que o compartilhamento inicial ocorreu em outra plataforma (ex: Facebook, Instagram etc)



Exemplo de boa rastreabilidade

Todas as URLs encontradas nos grupos são iguais (são encaminhamentos de um único “upload” original)

name	server-last-modified	mediaSize	mimeType
Zap-gabrielli-combina-bomba-folha-fakenews	Sat, 20 Oct 2018 18:33:28 GMT	72064	image/jpeg

DateTime	Sender	Group	mediaHash	URL
Sat, 20 Oct 2018 18:29:03 UTC	'+5521968762222	554784144486-1518054539@g.us	S0TWnOEIFZTLkKo2F3TI8ce3alQkq+tcUXI3C/75rRM=	https://mmg-fna.wh…p.net/d/f/At0iR1YjGIMJ2K9w
Sun, 21 Oct 2018 18:11:56 UTC	'+557199556868	557592231940-1526572162@g.us	S0TWnOEIFZTLkKo2F3TI8ce3alQkq+tcUXI3C/75rRM=	https://mmg-fna.w…p.net/d/f/At0iR1YjGIMJ2K9w
Sun, 21 Oct 2018 18:43:17 UTC	'+5515997721161	5521995194867-1538760042@g.us	S0TWnOEIFZTLkKo2F3TI8ce3alQkq+tcUXI3C/75rRM=	https://mmg-fna.whats…net/d/f/At0iR1YjGIMJ2K9w
Sun, 21 Oct 2018 19:30:57 UTC	'+553899393810	553884376163-1504388074@g.us	S0TWnOEIFZTLkKo2F3TI8ce3alQkq+tcUXI3C/75rRM=	https://mmg-fna.whatsapp.net/d/f/At0iR1YjGIMJ2K9w
Sun, 21 Oct 2018 19:38:13 UTC	'+553491933648	558393189100-1537154862@g.us	S0TWnOEIFZTLkKo2F3TI8ce3alQkq+tcUXI3C/75rRM=	https://mmg-fna.whatsapp.net/d/f/At0iR1YjGIMJ2K9w
Sun, 21 Oct 2018 23:13:55 UTC	'+5511944615724	554784144486-1518054632@g.us 'TROPA NACIONAL'	S0TWnOEIFZTLkKo2F3TI8ce3alQkq+tcUXI3C/75rRM=	https://mmg-fna.whatsapp.net/d/f/At0iR1YjGIMJ2K9w
Mon, 22 Oct 2018 01:59:49 UTC	'+5511994760407	558196526307-1504487534@g.us '(CDBr) Anti Comuna 2'	S0TWnOEIFZTLkKo2F3TI8ce3alQkq+tcUXI3C/75rRM=	https://mmg-fna.whatsapp.net/d/f/At0iR1YjGIMJ2K9w
Mon, 22 Oct 2018 10:27:18 UTC	'+553199097519	558799116313-1525037919@g.us 'Política presidencial'	S0TWnOEIFZTLkKo2F3TI8ce3alQkq+tcUXI3C/75rRM=	https://mmg-fna.whatsapp.net/d/f/At0iR1YjGIMJ2K9w
Mon, 22 Oct 2018 11:35:44 UTC	'+5511981798828	5511972315345-1497792293@g.us 'Política Brasil'	S0TWnOEIFZTLkKo2F3TI8ce3alQkq+tcUXI3C/75rRM=	https://mmg-fna.whatsapp.net/d/f/At0iR1YjGIMJ2K9w
Mon, 22 Oct 2018 12:07:14 UTC	'+554999115483	5517992100644-1523185260@g.us '@DireitaConservador #2'	S0TWnOEIFZTLkKo2F3TI8ce3alQkq+tcUXI3C/75rRM=	https://mmg-fna.whatsapp.net/d/f/At0iR1YjGIMJ2K9w
Mon, 22 Oct 2018 14:12:14 UTC	'+557788111622	5521995194867-1538247436@g.us	S0TWnOEIFZTLkKo2F3TI8ce3alQkq+tcUXI3C/75rRM=	https://mmg-fna.whatsapp.net/d/f/At0iR1YjGIMJ2K9w
Mon, 22 Oct 2018 16:43:42 UTC	'+5521965667277	556198294747-1535175456@g.us 'Brasil Ame-o ou Deixe-o!'	S0TWnOEIFZTLkKo2F3TI8ce3alQkq+tcUXI3C/75rRM=	https://mmg-fna.whatsapp.net/d/f/At0iR1YjGIMJ2K9w
Mon, 22 Oct 2018 19:01:51 UTC	'+556581523612	5517992100644-1518109036@g.us '@DireitaConservador #1'	S0TWnOEIFZTLkKo2F3TI8ce3alQkq+tcUXI3C/75rRM=	https://mmg-fna.whatsapp.net/d/f/At0iR1YjGIMJ2K9w
Mon, 22 Oct 2018 19:18:57 UTC	'+558599952529	558196526307-1507076270@g.us '(CDBr) Anti-Nova Ordem'	S0TWnOEIFZTLkKo…TI8ce3alQkq+tcUXI3C/75rRM=	https://mmg-fna.whatsapp.net/d/f/At0iR1YjGIMJ2K9w
Mon, 22 Oct 2018 20:13:54 UTC	'+5519992682222	554298091984-1483832784@g.us 'Apoiadores de Bolsonaro'	S0TWnOEIFZTLkK…TI8ce3alQkq+tcUXI3C/75rRM=	https://mmg-fna.whatsapp.net/d/f/At0iR1YjGIMJ2K9w
Mon, 22 Oct 2018 22:38:07 UTC	'+5511996590656	554784144486-1518065728@g.us 'Direita Conservador 1'	S0TWnOEIFZTLkKo…TI8ce3alQkq+tcUXI3C/75rRM=	https://mmg-fna.whatsapp.net/d/f/At0iR1YjGIMJ2K9w
Mon, 22 Oct 2018 23:34:38 UTC	'+557598921002	556185850997-1536286980@g.us	S0TWnOEIFZTLkK…2F3TI8ce3alQkq+tcUXI3C/75rRM=	https://mmg-fna.whatsapp.net/d/f/At0iR1YjGIMJ2K9w
Mon, 22 Oct 2018 23:40:10 UTC	'+5511995671227	558695748768-1526328559@g.us	S0TWnOEIFZTL…o2F3TI8ce3alQkq+tcUXI3C/75rRM=	https://mmg-fna.whatsapp.net/d/f/At0iR1YjGIMJ2K9w
Mon, 22 Oct 2018 23:56:18 UTC	'+5511999915794	554784144486-1518065728@g.us 'Direita Conservador 1'	S0TWnOEIFZTL…kKo2F3TI8ce3alQkq+tcUXI3C/75rRM=	https://mmg-fna.whatsapp.net/d/f/At0iR1YjGIMJ2K9w
Tue, 23 Oct 2018 00:03:19 UTC	'+557598625813	558695748768-1526328559@g.us	S0TWnOEIFZ…kKo2F3TI8ce3alQkq+tcUXI3C/75rRM=	https://mmg-fna.whatsapp.net/d/f/At0iR1YjGIMJ2K9w

A mídia é idêntica em todas as mensagens (mesmo “hash”).

Caminho para continuar a investigação (exemplo)

- Solicitar (via ordem judicial) ao WhatsApp os registros de acesso do usuário responsável pelo upload do arquivo que se encontra hospedado nos servidores da empresa na seguinte URL:

  https://mmg-fna.whatsapp.net/d/f/At0iR1YjGIMJ2K9wO80laYCThMKhTVq3frbzOqnNzdKt.enc

- Deve ser fornecidos os dados do terminal do usuário (número do telefone) e também dados de acesso (endereço IP) com data e hora.

Considerações finais

- Foram analisados 16 casos de “fake news” que circularam nos grupos de política, extraindo as URLs que permitiriam elaborar solicitações judiciais.
- É improvável que o WhatsApp ainda possua os registros de acesso da época, ainda mais considerando a resposta oficial da empresa sobre não guardá-los.
- O ajustamento de conduta da empresa quanto aos termos do Marco Civil permitiria que as autoridades pudessem realizar investigações de crimes na forma descrita.

Considerações finais

- Na opinião do autor, o mecanismo de rastreio aqui sugerido oferece uma janela segura para investigações moderadas, isto é, sem permitir abusos e o acesso em massa pelo Estado. Isto se aplicaria também a investigações de diferentes naturezas não eleitorais como, por exemplo, crimes de pedofilia. É necessário avançar com este debate na sociedade, reestabelecendo limites e deveres das empresas de tecnologia para que estas possam colaborar efetivamente com investigações legítimas sem violar os direitos individuais.