BRASIL

O Cenário das Ameaças Digitais: Sociedade Civil e Mídia

Internews
Local voices. Global change.

maria
[lab]

Índice

Contextualização

No Brasil, o crime cibernético é uma questão relevante que afeta todas as camadas da sociedade, com muitos cibercriminosos operando no país. Embora a sociedade civil esteja sujeita a muitas ameaças digitais, ataques mais avançados são menos comuns do que em outros países, como o México. Embora as ameaças direcionadas sejam menos comuns, elas ainda ocorrem e a sociedade civil deve ser proativa na segurança contra ameaças à sua segurança digital.

Este relatório foi preparado pela equipe de Liberdade e Resiliência na Internet da Internews seguindo um fluxo de trabalho que fortalece a capacidade de organizações da sociedade civil (OSC), jornalistas e outros defensores dos direitos humanos (DDH) de detectar, analisar e criar resiliência a ataques digitais por meio de expertise focada em análise de ameaças e resposta a incidentes. O presente relatório tem como objetivo fornecer uma visão geral das ameaças digitais enfrentadas pela sociedade civil e pela mídia no Brasil, bem como orientar os especialistas em segurança digital que apoiam essa comunidade. O relatório também apresenta um contexto para o setor de segurança cibernética, o qual pode precisar analisar incidentes de segurança que afetem a sociedade civil e os jornalistas brasileiros. Concluímos com uma discussão sobre medidas de mitigação que podem ser propostas por especialistas em segurança digital às pessoas e organizações com quem trabalham, além de poderem ser implementadas por organizações da sociedade civil.

Este relatório foi redigido em estreita colaboração com a MariaLab, uma associação independente e sem fins lucrativos que opera na intersecção entre política, gênero e tecnologia. A MariaLab trabalha para valorizar o autocuidado nas mídias digitais e levar a tecnologia aos espaços feministas e o feminismo aos espaços tecnológicos. A MariaLab constrói ambientes virtuais e físicos seguros, com dimensões sociais, étnicas ou econômicas; entendendo que somente assim o aprendizado pode ser construído por meio da troca e acúmulo de conhecimento entre todos.

As ameaças, as tendências e os estudos de caso destacados neste relatório foram identificados por meio de apoio direto à segurança digital para comunidades em risco (fornecido pela Internews e MariaLab), pesquisa documental e conversas com membros de confiança da comunidade *Internet Freedom*. Este relatório agrega dados do trabalho de resposta a incidentes e documenta padrões de ataque específicos do Brasil.

Outubro de 2023

Escrito e editado: Martijn Grooten, Ashley Fowler, Marc Shaffer e Skyler Sallick
Revisão, design e layout: Skyler Sallick

O Cenário das Ameaças Digitais

Contexto Político, Sociedade Civil e Mídia

O Brasil é um país democrático com eleições acirradas, como visto durante as eleições presidenciais de 2022, cujo resultado foi a retomada do cargo pelo ex-presidente Luiz Inácio Lula da Silva (conhecido simplesmente como Lula). Contudo, à medida que a extrema direita ganha popularidade e os políticos da extrema direita assumem cargos no governo, o Brasil passa por um retrocesso democrático, seguindo uma tendência global.[1] O Índice de Democracia do The Economist classifica o Brasil como uma "democracia imperfeita", atingindo a pontuação de 6,78 de 10, com uma pontuação semelhante a outros países das Américas, incluindo Argentina e Colômbia, e caindo na mesma categoria que os Estados Unidos.[2] O país é classificado como "Livre" no Relatório *Freedom in the World* de 2023 da Freedom House, com uma pontuação de 72 em 100,[3] em comparação com 79 em 2017.[4] A mudança mais significativa foi uma queda de seis pontos nas liberdades civis.

As comunidades vulneráveis no Brasil enfrentam ameaças significativas à sua segurança. Afro-brasileiros, brasileiros cujos ascendentes são predominantemente da África Subsaariana; mulheres; e a comunidade LGBTQ+ enfrentam ameaças ainda mais intensas. Apesar de muitas autoridades projetarem uma versão idealizada de igualdade racial, os afro-brasileiros sofreram discriminação há séculos, somente nos últimos anos foi que esforços foram feitos para reconhecer e corrigir as disparidades.[5] As mulheres também enfrentam ameaças significativas à sua segurança, conforme demonstrado por um relatório de 2022 do Fórum Brasileiro de Segurança que afirma que a violência contra as mulheres de todos os tipos tem aumentado.[6] A comunidade LGBTQ+ também corre riscos e pessoas que vivem na intersecção dessas identidades são as que mais sofrem, sendo o Brasil um dos países mais perigosos do mundo para mulheres trans negras.[7]

De acordo com a Freedom House, de modo geral, a sociedade civil consegue funcionar livremente no Brasil, porém, membros de organizações não governamentais, jornalistas e outros membros da sociedade civil sofrem assédio e violência, que aumentaram nos últimos anos. As grandes empresas podem exercer uma pressão significativa por meio da corrupção generalizada, afetando a capacidade dos ativistas de operarem livremente.[8] Tais empresas e o governo usam ameaças de difamação para controlar os meios de comunicação e, durante o governo do ex-presidente Bolsonaro, contas favoráveis ao governo nas redes sociais frequentemente publicavam informações pessoais de jornalistas na Internet sem a permissão deles. Jornalistas do sexo feminino são alvo de violência online com maior frequência, porém, devido a uma presença proporcionalmente baixa em cargos de alto nível nas organizações de comunicação social, essas questões não são levadas a sério.[9]

Jornalistas do sexo feminino são alvo de violência online com maior frequência, porém, devido a uma presença proporcionalmente baixa em cargos de alto nível nas organizações de comunicação social, essas questões não são levadas a sério.

No Brasil, diversos ativistas e jornalistas pagaram por seu ativismo com suas vidas.

No Brasil, diversos ativistas e jornalistas pagaram por seu ativismo com suas vidas. O indigenista brasileiro Bruno Pereira e o jornalista britânico Dom Philips foram assassinados enquanto viajavam para a segunda maior área indígena do país,[10] três ativistas ambientais da mesma família foram encontrados mortos no Pará[11] e um funcionário do então partido opositor Partido dos Trabalhadores (PT) foi morto a tiros por um apoiador de Bolsonaro.[12] Até políticos foram assassinados devido ao seu trabalho de promoção dos direitos humanos, o mais notável deles foi o assassinato de Marielle Franco. Marielle Franco, uma mulher negra, lésbica e da favela, foi vereadora no Rio de Janeiro. Ela provavelmente foi assassinada devido ao seu ativismo em nome dessas comunidades marginalizadas.[13] No governo de Bolsonaro, os investigadores e funcionários do governo não deram prioridade a esse assassinato e o caso continua sem solução. Com a eleição de Lula, a família de Marielle aguarda uma resolução.[14]

Segurança Cibernética no Brasil

À medida que as pessoas, organizações e empresas cada vez mais transferem suas operações para a Internet, as ameaças digitais, especialmente crimes cibernéticos com motivação financeira, têm efeitos cada vez mais prejudiciais. O crime cibernético no Brasil é um problema há bastante tempo, com muitos agentes anunciando abertamente suas atividades no Facebook e no Instagram. Os agentes de ameaças geralmente usam ferramentas e táticas como *malware* bancário e *phishing* para ganhar dinheiro, frequentemente visando o popular método de pagamento por "Boleto" com ataques de *phishing*.[15] Exemplos recentes de *malware* bancário também incluem as campanhas de *malware* Grandoreiro,[16] PixBankBot[17] e GeoMetrix[18].

O Brasil sofreu muitas violações de dados em que informações pessoais foram vazadas, inclusive de departamentos governamentais. Em 2018, um servidor mal configurado expôs a identificação de contribuinte de mais da metade da população e, em 2020, os dados pessoais de 16 milhões de pacientes com COVID-19 foram expostos na Internet.[19] Como apresentado no primeiro estudo de caso encontrado no Anexo B, os agentes de ameaça frequentemente usarão dados pessoais vazados em outros ataques.

Os cibercriminosos frequentemente invadem contas de e-mail e redes sociais para extorquir fundos dos proprietários das contas. Em 2023, a organização *Rest of World* informou que muitos acabam pagando "hackers éticos" para recuperar o acesso às suas contas do Instagram.[20] "Hacking", neste contexto, consiste em grande parte em navegar no complicado processo de atendimento ao cliente do Instagram, destacando falhas de usabilidade nos procedimentos padrão da Meta.

Apesar da prevalência do crime cibernético, o Brasil só adotou uma estratégia nacional de segurança cibernética em fevereiro de 2020.[21] Desde 2005, o governo brasileiro tem abordado questões de segurança cibernética como um aspecto da defesa nacional, levando à segurança cibernética militarizada; desde 2008, a segurança cibernética está sob a alçada das forças armadas. Entre 2012 e 2016, o Brasil sediou diversos eventos internacionais importantes, incluindo a Copa do Mundo FIFA de 2014 e os Jogos Olímpicos de 2016. Tais eventos levaram a um maior escrutínio e colocaram o governo sob intensa pressão para reforçar a sua segurança

cibernética. Todavia, as medidas adotadas não conseguiram fazer jus ao aumento da criminalidade cibernética. Alguns especialistas caracterizaram a política governamental desse período como uma "miragem".[22]

No final do mandato do presidente Michael Temer, o governo publicou a sua primeira estratégia nacional de segurança cibernética, o primeiro passo concreto para a melhoria. Em 2022, o Brasil aderiu à Convenção sobre o Crime Cibernético[i], facilitando o compartilhamento de provas eletrônicas de crimes cibernéticos com outros membros.[23] Essa Convenção é um dos principais mecanismos internacionais para esse tipo de compartilhamento.[24]

Com a crescente atenção dada à legislação em matéria de segurança cibernética, o equilíbrio entre a segurança cibernética e a proteção dos direitos digitais dos cidadãos tem sido objeto de um debate importante. As OSC e outros defensores apontaram para um aumento na vigilância e um enfraquecimento da privacidade online.[25] Atualmente, o governo brasileiro está debatendo uma proposta de Lei das Fake News, formalmente conhecida como Projeto de Lei 2.630,[26] que exigiria que as empresas de internet "encontrassem e denunciassem materiais ilegais, em vez de deixar essa tarefa a cargo dos tribunais". O não cumprimento dessa exigência resultará em multas altas.[28] A lei enfrenta oposição significativa de empresas de tecnologia, incluindo Google e Meta, enquanto a sociedade civil parece dividida sobre o projeto de lei. Os apoiadores do projeto argumentam que ele serve como uma medida necessária para neutralizar o aumento da atividade ilegal online. Entretanto, os críticos argumentam que o projeto de lei foi criado às pressas após a invasão de prédios do governo por apoiadores de Bolsonaro após sua derrota nas eleições de 2022. Segundo os críticos, o projeto de lei representa uma ameaça à privacidade e aumenta o potencial de vigilância.

De acordo com a empresa de segurança cibernética Torchlight, mesmo com a promulgação da nova legislação pelo governo, o cenário regulatório da segurança cibernética ainda precisa de coesão. Ainda há vulnerabilidades que podem ser exploradas e as empresas ainda precisam investir muito em medidas de segurança cibernética.[29] Nos últimos anos, as empresas aumentaram sua demanda por apólices de seguro cibernético no Brasil e estima-se que os gastos com segurança cibernética tenham ultrapassado um bilhão de dólares norte-americanos pela primeira vez.[30] A pandemia da COVID-19 aumentou a necessidade de segurança cibernética à medida que as empresas se digitalizavam cada vez mais em resposta à pandemia.

Além dos ataques cibernéticos e das vulnerabilidades legislativas, a vigilância governamental também é uma preocupação crescente no Brasil. Na década anterior, diversos órgãos de inteligência militar e civil brasileiros discutiram sobre a compra do spyware da Hacking Team.

Além dos ataques cibernéticos e das vulnerabilidades legislativas, a vigilância governamental também é uma preocupação crescente no Brasil. Na década anterior, diversos órgãos de

[i] A Convenção sobre o Crime Cibernético, ou Convenção de Budapeste, é uma iniciativa do Conselho da Europa descrita como uma "**estrutura que permite a centenas de profissionais das Partes compartilhar experiências e criar laços que facilitam a cooperação** em casos específicos, inclusive em situações de emergência, para além das disposições específicas previstas nesta Convenção."

inteligência militar e civil brasileiros discutiram sobre a compra do *spyware* da Hacking Team.[31] Apenas um deles foi confirmado como cliente, a Polícia Federal do Brasil. Não se sabe se e como eles usaram o *spyware*. Em 2021, o governo brasileiro supostamente negociou com a empresa israelense de vigilância digital NSO Group a aquisição de seu principal *spyware,* o Pegasus.[32] Carlos Bolsonaro, vereador do Rio de Janeiro e filho do então presidente Jair Bolsonaro, participou dessas negociações. Não ficou claro se o Brasil comprou o Pegasus e, se o fez, se ele foi usado. Nenhum sinal do Pegasus foi encontrado no país. No entanto, de acordo com um relatório do Instituto de Pesquisa em Direito e Tecnologia do Recife (IP.rec), o governo "legitimou" com sucesso o uso de software de vigilância e essas ferramentas foram assimiladas na prática geral.[33]

Condição da Segurança Cibernética da Sociedade Civil e da Mídia

Assim como outras comunidades no Brasil, a sociedade civil e a mídia enfrentam diversas ameaças à sua segurança cibernética, porém, as OSC e as organizações de mídia enfrentam o risco adicional de ataques e retaliação.

O impacto psicológico até mesmo do crime cibernético mais simples sobre as pessoas em risco, especialmente as mulheres e as pessoas da comunidade LGBTQ+, pode ser enorme.

A sociedade civil no Brasil não está imune aos ataques com motivação financeira que afetam muitas pessoas no país, com diversos ativistas perdendo dinheiro em decorrência de fraudes digitais. Isso não causa apenas um impacto financeiro em grupo que já precisa de dinheiro; membros da sociedade civil podem ficar traumatizados pela experiência. Os ativistas podem ter dificuldade em determinar se os ataques são dirigidos contra eles, o que pode levar a um stress significativo e ao medo da vigilância. Como mostra o estudo de caso apresentado no Anexo C, o impacto psicológico até mesmo do crime cibernético mais simples sobre as pessoas em risco, especialmente as mulheres e as pessoas da comunidade LGBTQ+, pode ser enorme.

Muitos mercenários imersos no setor de vigilância, ou "hackers de aluguel", atuam no Brasil e têm como alvo funcionários do governo e jornalistas. Os investigadores encontraram provas de que grupos criminosos nacionais e internacionais operam no Brasil. Em 2016, a empresa de segurança cibernética Kaspersky informou sobre o "Grupo Poseidon", um grupo de ataque direcionado provavelmente baseado fora do Brasil. O Grupo Poseidon é especializado em espionagem e as evidências demonstram que sua operação pode ter tido início, no mínimo, em 2001. O Poseidon geralmente tenta roubar propriedade intelectual e informações comerciais, porém, foi demonstrado que eles também atacam jornalistas.[34] Sabe-se que esses criminosos permanecem fora do radar durante anos e, por isso, é difícil saber a extensão das suas operações. Os profissionais de segurança cibernética também provaram que os cibercriminosos têm o Brasil como um alvo. Um desses grupos é o "Void Balaur", um grupo de cibermercenários provavelmente sediado no Leste da Europa que tem uma ampla gama de alvos e fornece diversos serviços, incluindo a coleta de dados privados e o acesso a contas.[35] Foi comprovado que seus alvos são políticos e jornalistas. A empresa de segurança SentinelOne relata pelo menos um alvo no Brasil, sem fornecer mais detalhes.[36]

Do ponto de vista do operador, os "bons" spywares e os "bons" hacks, em geral, não são descobertos pelo alvo. E embora nenhum spyware seja perfeito, quanto menos pessoas o procurarem ativamente, menor será a probabilidade de ele ser descoberto. A sociedade civil brasileira, como em muitas outras partes do mundo, geralmente não os procura ativamente, como por meio de auditorias direcionadas ou do uso de software de segurança avançado.

Há pouquíssimas evidências de que o governo brasileiro use o *spyware* da Hacking Team ou o Pegasus para atingir a sociedade civil. Isso pode ser de certo modo surpreendente dada a sua prevalência em outros países latino-americanos, sendo o México um exemplo particularmente notório. Em geral, apenas governos e militares podem adquirir *spyware* avançado. Em termos globais, esses órgãos utilizaram o software contra a sociedade civil sob o pretexto de proteger a segurança nacional, mesmo que a motivação para a sua utilização seja baseada em outros fatores, como a corrupção, o ataque à oposição pela extrema direita ou a retaliação contra jornalistas e ativistas. Embora as evidências do uso de *spyware* avançado no Brasil sejam limitadas, a possibilidade de seu uso no futuro ainda é preocupante e merece atenção redobrada.

Do ponto de vista do operador, os "bons" *spywares* e os "bons" hacks, em geral, não são descobertos pelo alvo. E embora nenhum *spyware* seja perfeito, quanto menos pessoas o procurarem ativamente, menor será a probabilidade de ele ser descoberto. A sociedade civil brasileira, como em muitas outras partes do mundo, geralmente não os procura ativamente, como por meio de auditorias direcionadas ou do uso de software de segurança avançado. Por enquanto, sua existência no Brasil não deve ser descartada como uma possibilidade.

Medidas de Mitigação

Para ajudar ainda mais a sociedade civil brasileira a compreender toda a extensão dos ataques digitais, recomenda-se mais **recursos para auditorias**, em particular auditorias que incluam análise forense de dispositivos, e **software de segurança**.

A segurança da conta é importante para qualquer pessoa no Brasil e para membros da sociedade civil e da mídia em particular. A **autenticação de duplo fator é essencial** e atenua o uso menos controlável de senhas fracas e/ou reutilizadas. Embora seja melhor do que nenhum segundo fator, o SMS não deve ser considerado seguro, especialmente para usuários de risco. Aplicativos de autenticação são melhores, ao passo que o uso de tokens de hardware, de modo geral, oferece a melhor segurança.

Alguns aplicativos de mensagens, como Telegram, WhatsApp e Signal, exigem o uso de um número de telefone para ativar a conta. A habilitação da autenticação de duplo fator **adiciona uma senha** além do uso de SMS para acessar a conta, proporcionando segurança em casos de comprometimento do SMS. Quando esse recurso estiver habilitado, o aplicativo solicitará periodicamente ao usuário que insira sua senha para garantir que as mensagens não estão sendo acessadas por terceiros além do proprietário da conta. Isso evita a aquisição do controle de contas por meio de interceptação de SMS, algo comum no país.

Os dispositivos, como laptops e telefones celulares, devem estar sempre atualizados aplicando patches de segurança aos sistemas operacionais e outros softwares sempre que estiverem disponíveis. **Softwares só devem ser adquiridos de fontes oficiais**, o que, em muitos casos, exigirá pagamento. As ONGs não devem ter vergonha de discutir essa questão com seus financiadores ou de procurar alternativas gratuita, seja através de software de código aberto ou através de programas que forneçam o software gratuitamente ou a preços reduzidos para ONGs qualificadas. Para organizações que buscam soluções de longo prazo ou mais autossustentáveis é essencial contratar ou ter parceria com profissionais de TI. Com pessoal adequado, as organizações conseguirão configurar e manter sua própria infraestrutura com foco na segurança e proteção de dados. As soluções técnicas, incluindo os tipos de software utilizados, irão variar dependendo das necessidades e dos recursos da organização.

No Brasil, a FASE – Federação de Órgãos para Assistência Social e Educacional desenvolveu um relatório que analisou a conexão entre filantropia e segurança digital. Esse relatório fornece mais informações para organizações da sociedade civil que buscam se conectar com doadores que poderiam financiar melhorias na segurança digital, além de informações para doadores que visam ajudar a melhorar a segurança digital da sociedade civil no Brasil.

Embora não se saiba se a sociedade civil do país foi alvo de *spyware* avançado, como o Pegasus, alvos considerados de alto valor devem se atentar a esse tipo de *spyware,* o qual, normalmente, explora vulnerabilidades de dia zero e ataques de zero clique. Esses tipos de ataques significam que um dispositivo completamente corrigido pode ser atacado de uma forma que o usuário não consegue prevenir evitando um link ou anexo suspeito. Isso deve ser levado em consideração por aqueles que correm riscos devido a esse tipo de *spyware*.

Os alvos potenciais são incentivados a **usar mensagens temporárias** em aplicativos de mensagens, em cujo caso as mensagens são excluídas automaticamente após um determinado período, pois isso pode limitar os danos de um futuro comprometimento da conta. A compartimentalização, por meio do **uso de dispositivos separados para trabalho e uso pessoal**, ou até mesmo um **dispositivo separado para trabalhos de alto risco**, também limita os danos, contudo, isso acarreta custos e inconveniências adicionais.

Manter os dispositivos atualizados é muito importante e, em iPhones, **reinicializar os dispositivos regularmente**, de preferência uma vez por dia, e usar o **modo Lockdown da Apple** também reduz a probabilidade de ataques.

Com relação a dispositivos Android, sabe-se muito menos sobre *spywares* direcionados a eles, embora isso não signifique que os usuários do Android corram menos riscos. Dispositivos Android mais caros, incluindo os dispositivos Pixel do Google, são mais seguros e, geralmente, recebem correções de vulnerabilidades mais rapidamente do que dispositivos Android mais baratos. A reinicialização regular dos dispositivos provavelmente reduzirá danos, pois o *spyware* geralmente é removido dos dispositivos após a reinicialização.[ii] Reiniciar um dispositivo Android também pode remover evidências de um ataque anterior, o que pode ser uma preocupação para alguns usuários.

[ii] Esse é o caso de todos os *spywares* conhecidos para iPhone e, provavelmente, também de *spywares* para Android, especialmente aqueles que fazem *root* no dispositivo.

Por fim, a maioria das ameaças enfrentadas pela sociedade civil e pela mídia no Brasil não são sofisticadas e são bem-sucedidas porque os alvos podem não ter conhecimento quando se trata de tecnologia. Os recursos para melhoria da segurança devem proporcionar oportunidades para toda a comunidade aprender mais sobre tecnologia e segurança digital, em vez de apenas obter informações sobre ameaças avançadas.

Estudos de Caso

Estudo de Caso de Extensão de Navegador Não Autorizada

Uma organização da sociedade civil brasileira especializada em litígios em casos de violação de direitos humanos utiliza o software de segurança Malwarebytes, o qual visa detectar *malware* em dispositivos. Esse software é gerenciado de modo centralizado, algo bastante incomum em organizações menores da sociedade civil, e o administrador recebeu um alerta de que um "*spyware*" foi detectado em um dos dispositivos.

A análise do alerta e a investigação do laptop afetado levaram à descoberta de uma extensão de navegador "Netflix party", que foi anunciada como uma possibilidade para que vários usuários assistissem à Netflix juntos. O usuário confirmou que, de fato, instalou tal extensão, mas que isso foi feito em seu laptop pessoal. No entanto, como o usuário estava conectado ao Chrome em seu laptop pessoal e de trabalho, o Chrome sincronizou automaticamente as extensões de modo que a extensão maliciosa também apareceu no laptop de trabalho. Esse tipo de sincronização provavelmente não é algo que muitas pessoas conheçam. Isso poderia facilmente anular alguns dos benefícios da separação de dispositivos de trabalho e pessoais, enfatizando a necessidade de treinamento em segurança da informação.

A Marialab, uma associação independente sem fins lucrativos que opera na intersecção de política, gênero e tecnologia, conduziu uma breve análise do plugin e descobriu que ele enviava todos os URLs visitados para o servidor de comando e controle do plugin e executava ações adicionais dependendo da resposta do servidor para ganhar dinheiro por meio de esquemas de afiliados.

Essa pesquisa corresponde ao que a empresa de segurança McAfee escreveu em uma análise de cinco extensões maliciosas do Chrome publicada em agosto de 2022.[37] As extensões incluíam "Netflix Party" e "Netflix Party 2", ambas estavam presentes no laptop afetado.

Para fazer a limpeza, a extensão foi desinstalada e todos os arquivos que o Malwarebytes detectou como maliciosos foram removidos manualmente. As entradas do registro criadas pelo plugin também foram removidas, pois o Malwarebytes também as sinalizou.

Aqui, deve-se observar que não é incomum que softwares de segurança detectem arquivos individuais vinculados a uma infecção como maliciosos, mesmo que, por si só, os arquivos não fossem capazes de causar qualquer dano. Esse foi o caso discutido, uma vez que a própria extensão foi desinstalada. Geralmente, é uma boa ideia remover todos os arquivos sinalizados como maliciosos.

Após remover esses arquivos, uma nova verificação mostrou que o computador estava limpo. Foi recomendado ao usuário usar um navegador diferente, neste caso, o Firefox, para fins de trabalho.

Extensões para o Chrome e outros navegadores podem melhorar significativamente a experiência do usuário no navegador. Porém, tais extensões têm muito poder, como acesso a todos os dados do navegador, incluindo URLs visitados e possíveis cookies.

Como foi o caso aqui discutido, elas podem ser usadas pelos desenvolvedores da extensão para ganhar dinheiro por meio de esquemas de afiliados, algo que tem um impacto relativamente baixo sobre o próprio usuário. No entanto, elas também podem ser usadas para sequestrar sessões, por exemplo, de webmail e serviços financeiros. Esse sequestro de sessão é eficaz mesmo se o usuário utilizar autenticação multifatorial forte para proteger a conta e pode levar ao roubo de dados pessoais ou dinheiro.

Os usuários em risco devem pensar com muito cuidado ao instalar extensões de navegador. Idealmente, apenas extensões de desenvolvedores verificados e confiáveis seriam instaladas. Em caso de dúvida, caso uma extensão seja necessária, possíveis danos podem ser mitigados instalando a extensão em um navegador diferente do principal utilizado.

Estudo de Caso da Ativista que Recebeu E-Mail de Sextorsão Personalizado

Em outubro de 2022, no Brasil, uma ativista recebeu um e-mail preocupante. Escrito em português fluente, o e-mail mencionava seu nome completo, endereço de e-mail e uma de suas senhas. Além disso, mencionava que o remetente havia instalado *spyware* na máquina e publicaria detalhes de sua atividade online e gravações de sua webcam, a menos que ela pagasse R$ 3.000,00 (pouco mais de US$ 600,00) para um endereço Bitcoin específico.

Embora seja um montante pequeno no contexto dos valores envolvidos em crimes cibernéticos e *ransomware*, é um montante elevado para um indivíduo, mais de um terço da renda média mensal do país.

E, embora receber um e-mail ameaçador como esse seja preocupante para qualquer pessoa, trata-se de uma preocupação especial para alguém cujas atividades online a tornam alvo de diversos tipos de assédio. Além disso, a sexualização das mulheres online torna o possível vazamento de informações e imagens pessoais ainda mais problemático.

A ativista entrou em contato com a parceira da Internews, MariaLab, uma associação independente sem fins lucrativos, que opera na interseção de política, gênero e tecnologia. Eles analisaram o e-mail e confirmaram que, apesar da inclusão de dados pessoais, ele não era de forma alguma direcionado a ela. Na verdade, tal e-mail foi um exemplo de uma fraude comum que remonta pelo menos a 2018.[38]

Os dados pessoais incluídos nesse caso provêm de uma violação de dados, que permite aos golpistas enviar e-mails "personalizados" como esse em larga escala, às vezes até milhões de e-mails por campanha. Usando o site "Have I Been Pwned", que monitora violações de dados, a

MariaLab conseguiu confirmar que o endereço de e-mail da ativista estava entre nada menos do que três violações de dados.

Convencida de que não se tratava de uma tentativa real de extorsão, ela não pagou os três mil reais. Entretanto, o mesmo endereço Bitcoin recebeu 20 pagamentos na mesma época, sugerindo que algumas pessoas caíram no golpe. A Marialab aproveitou a oportunidade para ajudar a ativista a proteger melhor seus dispositivos e contas.[39]

Golpes de "sextorsão" como esses são comuns e são um exemplo de crime cibernético de baixo nível. Contudo, esse caso, que não é único entre ativistas da sociedade civil e jornalistas, mostra que esses golpes ainda podem ter um impacto muito grande em certas pessoas em risco.

O *spyware* é uma ameaça real e o *spyware* que rouba informações que são posteriormente usadas para extorsão existe, mas é extremamente raro. O acesso de *malware* à câmera é muito raro em laptops modernos, embora, para maior tranquilidade, não custe nada usar um protetor de webcam quando não estiver utilizando a câmera ativamente. Alguns laptops possuem um protetor integrado.

Há pouco que se possa fazer para evitar que informações pessoais fornecidas a terceiros sejam roubadas em uma violação de dados, embora, felizmente, o armazenamento de senhas tenha melhorado muito nos últimos anos, de modo que vazamentos incluindo senhas estão se tornando menos comuns. A maioria dos e-mails de sextorsão envolve violações de dados de muitos anos atrás.

Há vários bons motivos para usar senhas exclusivas para cada serviço e utilizar um gerenciador de senhas pode ajudar a controlá-las. Nesse caso, se a senha usada para extorsão for exclusiva e usada apenas em um site ou plataforma, o alvo desse e-mail saberá de onde veio a violação.

Leitura Complementar

Tal como se observa neste relatório, as organizações da sociedade civil e os jornalistas frequentemente enfrentam ameaças únicas e avançadas, ao mesmo tempo em que carecem de recursos para as detectar, analisar e prevenir essas ameaças. Uma compreensão profunda das ameaças que a sociedade civil e a mídia enfrentam permite aos profissionais de segurança digital adaptar as suas respostas e apoiar melhor as organizações com as quais trabalham, levando a medidas de mitigação personalizadas que são mais eficientes e mais fáceis de serem implementadas por organizações da sociedade civil e da mídia. Para obter mais informações sobre as ameaças enfrentadas pela sociedade civil e pelos jornalistas, a Internews e seus parceiros elaboraram o relatório "Tendências Globais em Ameaças Digitais: Sociedade Civil e Mídia", bem como Relatórios sobre o Panorama das Ameaças Digitais para Armênia, México, Sérvia e Ucrânia. Esses recursos podem ser encontrados na página Technology Resources da Internews.

História do Brasil

A República Federativa do Brasil é uma república federal constitucional presidencialista na América do Sul, o maior país do continente. O Brasil também é o quinto maior país do mundo em termos de área e o sétimo mais populoso. O Brasil é membro de várias organizações internacionais de grande porte, incluindo as Nações Unidas,[40] o G20,[41] o BRICS,[42] o Mercosul[43] e a Organização dos Estados Americanos.[44] Originalmente habitado por vários grupos indígenas, o Brasil foi colonizado pelos portugueses no início do século XVI antes de se tornar um país independente em 1822 como o Império do Brasil. O Império do Brasil adotou uma constituição em 1824, a qual estabeleceu uma monarquia constitucional com legislatura bicameral. Em 1889, após a abolição da escravatura, os militares lideraram um golpe de Estado que reformou o governo para uma república presidencialista. O Brasil ficou sob regime militar autoritário de 1964 a 1985, durante o qual violações dos direitos humanos e execuções extrajudiciais eram comuns. Em 1985, o governo civil foi restabelecido e a atual constituição foi adotada em 1988.[45]

Agradecimentos

Desde 2021, a Internews trabalha com sete *Threat Labs* (*organizações locais com capacidade técnica e ferramentas apropriadas para analisar amostras suspeitas de* phishing *e* malware *e depois compartilhar informações com a comunidade sobre tendências de ataques, ameaças emergentes e contramedidas*) para responder a incidentes que afetam a segurança digital de organizações da sociedade civil e de mídia em todo o mundo. Os dados coletados por meio do programa de resposta a incidentes ajudaram a moldar abordagens de mitigação e resposta para comunidades em risco e serviram de base para este relatório.

A Internews gostaria de expressar sua gratidão à comunidade de *Threat Labs* que trabalhou conosco neste projeto. Eles estão empenhados em ajudar os necessitados e em garantir que seus parceiros da sociedade civil e das organizações de mídia possam concluir seu importante trabalho com segurança e efetividade. No total, este projeto apoiou *Threat Labs* na resposta a mais de 200 incidentes de segurança digital e na publicação de mais de 60 recursos educativos por meio de seus websites e plataformas de redes sociais.

Gostaríamos de fazer um agradecimento especial à MariaLab pelo fornecimento de informações para documentar e compartilhar esses estudos de caso e pela revisão e contribuição com feedback valioso para este relatório. O relatório não teria sido possível sem a sua cooperação e experiência.

Notas de rodapé

[1] "Democracy Index 2022." Economist. Acessado em julho de 2023. https://www.eiu.eom/n/campaigns/democracy-index-2022/.

[2] "Democracy Index 2022," Economist.

[3] "Freedom in the World 2023: Brazil." Freedom House. Acessado em julho de 2023. https://freedomhouse.org/country/brazil/freedom-world/2023.

[4] "Freedom in the World 2017: Brazil." Freedom House. Acessado em julho de 2023. https://freedomhouse.org/country/brazil/freedom-world/2017/.

[5] "Afro-Brazilians." Minority Rights Group International, World Directory of Minorities and Indigenous Peoples. Acessado em julho de 2023. https://minorityrights.org/minorities/afro-brazilians/.

[6] Viapiana, Tabata. "In Brazil, 14 women are physically assaulted per minute: new study." Brazil Reports. 8 de março de 2023. https://brazilreports.com/in-brazil-14-women-are-physically-assaulted-per-minute-new- study/4157/.

[7] Damasceno, Edilana. "8 Every 10 Black and LGPTGIAP+ People Have Been Victims of Hate Speech." Data Labe. 29 de março de 2023. https://datalabe.org/iea negres lgbtqiap/.

[8] "Freedom in the World 2023: Brazil," Freedom House.

[9] "UNESCO in Brazil shows the scenario of violence against women journalsits." UNESCO, News. Última atualização em 20 de abril de 2023. https://www.unesco.org/en/articles/unesco-brazil-shows-scenario-violence- against-women-journalists.

[10] Vieira, Matheus. "Brazil: Amnesty International laments brutal deaths of Bruno and Dom and demands justice." Amnesty International. 16 de junho de 2022. https://www.amnesty.org/en/latest/news/2022/06/brazil-amnesty-laments-brutal-deaths-bruno-dom-demands-justice/.

[11] "Americas: Amnesty International sounds alter over killings of human rights defenders and journalists in first month of 2022." Amnesty International. 2 de fevereiro de 2022. https://www.amnesty.org/en/latest/news/2022/02/americas-alert-killings-human-rights-defenders-journalists/.

[12] Mano, Ana. "Brazil party official shot dead as pre-election political violence escalates." Reuters. Última modificação em 11 de julho de 2022. https://www.reuters.com/world/americas/brazil-party-official-shot-dead-pre- election2poJjtica-vio]enceLescaJates-2022-07z10/.

[13] De Mattos Rocha, Lia. "The life and battles of Marielle Franco." openDemocracy. 20 de março de 2019. https://www.opendemocracy.net/en/democraciaabierta/life-and-battles-marielle-franco/.

[14] Carvalho, Igor. Rocha, Ana Paula, trans. "Marielle's murder: 'My mom should be remembered for her work, not for the unsolved crime.'" Brasil de Fato. 14 de março de 2023. https://www.brasildefato.com.br/2023/03/14/marielle-s-murder-my-mom-should-be-remembered-for-her-work-not-for-the-unsolved-crime.

[15] "Boleto malware may lost Brazil $3.75bn." *BBC*. Última modificação em 3 de julho de 2014. https://www.bbc.com/news/technology-28145401.

[16] Bautista, Bernard. "Grandoreiro Banking Malware Resurfaces for Tax Season." Trustwave. 26 de maio de 2022. https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/grandoreiro-banking-malware- resurfaces-for-tax-season/.

[17] "PixBankBot: New ATS-Based Malware Poses Threat to the Brazilian Banking Sector." Cyble. 30 de maio de 2023. https://cyble.com/blog/pixbankbot-new-ats-based-malware-poses-threat-to-the-brazilian-banking- sector/.

[18] Lytzki, Igal. "Operation Geometrix Do Brazil." Perception Point. 25 de julho de 2023. https://perception-point.io/blog/operation-geometrix-do-brasil/.

[19] Shoorbajee, Zaid. "Misconfigured server exposed half of all Brazilian taxpayer ID numbers, report says." *CyberScoop*. 11 de dezembro de 2018. https://cyberscoop.com/brazil-data-breach-cpf-120-million-infoarmor/.

[20] Dib, Daniela and Marflia Marasciulo. "Instagram account hacked? 'Ethical hackers' will get it back." *Rest of World*. 21 de agosto de 2023. https://restofworld.org/2023/hacked-instagram-account-recovery-ethical-hackers/.

[21] Hurel, Louise Marie. "Brazil's First National Cybersecurity Strategy: An Analysis of its Past, Present and Future." School of Public Policy at Georgia Institute of Technology, Internet Governance Project. 5 de abril de 2020. https://www.intemetgovemance.org/2020/04/05/brazils-first-national-cybersecurity-strategy-an-analysis-of-its-past-present-and-future/.

[22] Hurel, "Brazil's First National Cybersecurity Strategy: An Analysis of its Past, Present and Future."

[23] "Brazil accedes to the Convention on Cybercrime and six States sign the new Protocol on e-evidence." Council of Europe, Cybercrime, News. 30 de novembro de 2022. https://www.coe.int/en/web/cybercrime/-/brazil-accedes-to-the-convention-on-cybercrime-and-six-states-sign-the-new-protocol-on-e-evidence.

[24] Bannelier, Karine. "The U.N. Cybercrime Convention Should Not Become a Tool for Political Control or the Watering Down of Human Rights." *Lawfare*. 31 de janeiro de 2023. https://www.lawfaremedia.org/article/the-u.n.-cybercrime-convention-should-not-become-a-tool-for-political-control-or-the-watering-down-of-human-rights.

[25] Bannelier, "U.N. Cybercrime Convention Should Not Become a Tool for Political Control or the Watering Down of Human Rights."

[26] PL 2630/2020. Camara dos Deputados. https://www.camara.leg.br/propostas-legislativas/2256735

[27] Boadle, Anthony. "Brazil pushes back on big tech firms' campaign against 'fake news law'." *Reuters*. 2 de maio de 2023. https://www.reuters.com/world/americas/brazil-lawmakers-vote-controversial-bill-clean-up- social-media-2023-05-02/.

[28] Ibid.

[29] "Illuminate Your Unknowns." Torchlight AI. Acessado em julho de 2023. https://www.torchlight.ai/illuminate-your-unknowns/.

[30] "Illuminate Your Unknowns," Torchlight AI.

[31] Antonialli, Dennys e Jacqueline de Souza Abreu. "State Surveillance of Communications in Brazil and the Protection of Fundamental Rights." Electronic Frontier Foundation and Internet Lab. Dezembro de 2015. https://www.eff.org/files/2015/12/17/brazil-en-dec2015 0.pdf.

[32] "Brazil: Million-dollar negotiation for the Pegasus espionage programme, developed by the NSO Group, excluded official government investigation bodies that would directly benefit from the tool." Business & Human Rights Resource Centre. 8 de junho de 2021. https://www.business-humanrights.org/en/latest-news/brazil-million-dollar-negotiation-for-the-pegasus-espionage-programme-developed-by-the-nso-group-excluded-official-government-investigation-bodies-that-would-directly-benefit-from-the-tool/.

[33] Andre Ramiro, Pedro Amaral, Mariana Canto e Marcos Cesar M. Pereira. "Insecurity merchants: conjuncture and risks of governmental hacking in Brazil." https://ip.rec.br/publicacoes/mercadores-da-inseguranca-conjuntura-e-riscos-do-hacking-governamental-no-brasil/

[34] "Poseidon Group: a Targeted Attack Boutique specializing in global cyber-espionage." SecureList. 9 de fevereiro de 2016. https://securelist.com/poseidon-group-a-targeted-attack-boutique-specializing-in-global-cyber-espionage/73673/.

[35] "Void Balaur and the Rise of the Cybermercenary Industry." Trend Micro Research. 10 de novembro de 2021. https://www.trendmicro.com/en_us/research/21/k/void-balaur-and-the-rise-of-the-cybermercenary-industry.html.

[36] Hegel, Tom. "Void Balaur: The Sprawling Infrastructure of a Careless Mercenary." SentinelLABS. 22 de setembro de 2022. https://www.sentinelone.com/labs/the-sprawling-infrastructure-of-a-ca reless-mercenary/.

[37] "Malicious Cookie Stuffing Chrome Extensions with 1.4 Million Users." McAfee Labs. 29 de agosto de 2022. https://www.mcafee.com/blogs/other-blogs/mcafee-labs/malicious-cookie-stuffing-chrome-extensions-with-1-4-million-users/.

[38] "Sextortion Scam Uses Recipient's Hacked Passwords." KrebsonSecurity. 12 de julho de 2018. https://krebsonsecurity.com/2018/07/sextortion-scam-uses-recipients-hacked-passwords/.

[39] "38pnj-nLRXW." Blockchain.com. Acessado em julho de 2023. https://www.blockchain.com/explorer/addresses/btc/38pnj1L9gKLhYWTqGYBTkY2LroM2nnLRXW.

[40] "Member States." Nações Unidas. Acessado em julho de 2023. https://www.un.org/en/about-us/member-states.

[41] "About G20." Grupo dos Vinte. Acessado em julho de 2023. https://www.g20.org/en/about-g20/.

[42] du Plessis, Carien, Anait Miridzhanian, and Bhargav Acharya. "BRICS welcomes new members in push to reshuffle world order." *Reuters*. 24 de agosto de 2023. https://www.reuters.com/world/brics-poised-invite-new-members-join-bloczsources-2023-08-24/.

[43] "MERCOSUR Countries." MERCOSUL. Acessado em julho de 2023. https://www.mercosur.int/en/about-mercosur/mercosur-countries/.

[44] "Member States." OEA Acessado em julho de 2023. https://www.oas.org/en/member states/default.asp.

[45] "Brazil country profile." *BBC*. Última modificação em 2 de junho de 2023. https://www.bbc.com/news/world-latin-america-18909529.