Edital do "Programa Malhas Digitais" para financiamento de projetos de construção de protocolos para detecção de spywares no Brasil

A Associação Data Privacy Brasil de Pesquisa ("Data Privacy Brasil"), organização sem fins lucrativos registrada em São Paulo, torna público o Edital do "Programa Malhas Digitais" para financiamento de projetos de construção de protocolos para detecção de spywares no Brasil, conforme as disposições abaixo. O Edital tem por objetivo apresentar as condições de submissões de projetos de **até R$ 50.000,00** (cinquenta mil reais), que devem ser submetidos até **31 de outubro de 2024**.

Apoiado pelo projeto internacional *Spyware Accountability Initiative*, o Programa Malhas Digitais tem como objetivo criar uma estrutura de financiamento semente, com apoio financeiro e profissional em ciência da computação, para projetos iniciais com capacidade de produção de protótipos para detecção de spywares no Brasil, criando condições iniciais de monitoramento ativo de detecções para preservação de direitos fundamentais.

Atenção: sugerimos **ler o edital completo**. Se restarem dúvidas, escreva para pesquisa@dataprivacybr.org.

1. Definições iniciais: spywares e métodos de detecção

1.1. Spywares são, em linhas gerais, ferramentas (*softwares*) com capacidades intrusivas de extração de informações e invasão em dispositivos ou sistemas eletrônicos e de comunicações, construídos a partir da exploração de falhas de segurança que eventualmente existam nesses dispositivos ou em redes e protocolos de informação por meio dos quais transitam os fluxos de comunicação. O usuário, titular ou operador do sistema dificilmente é capaz de ter conhecimento a respeito da instalação de um spyware, uma vez que essas ferramentas são intencionalmente construídas com o objetivo de serem silenciosas.

1. 2. Os diferentes tipos de spywares precisam passar por quatro elementos comuns, que os tornam identificáveis como tal: (i) os dados são obtidos de um dispositivo a partir de uma extração que não ocorreria se não fosse em razão da introdução de um programa de

computador, código ou ataque; (ii) os dados são extraídos dos dispositivos partindo da premissa de que o usuário do dispositivo tido como alvo não está ciente da situação de extração de informações; (iii) o código ou programa de computador é utilizado no contexto de criar um alvo, seja um indivíduo ou um grupo de indivíduos, com a intenção de monitoramento, rastreio e vigilância; (iv) os dados que são extraídos dos dispositivos possuem um contexto específico legítimo e podem ser considerados como informações privadas, como localização, fotos, senhas, mensagens, metadados de aplicativos, entre outros.

1. 3. Conforme argumentado pela Data Privacy Brasil e o InternetLab no curso da ADPF 1143, em julgamento no Supremo Tribunal Federal, entendemos que os spywares podem ser de diferentes tipos, como spywares de: extração em dispositivo; extração em infraestrutura; derrubada de chaves criptográficas; extração de informações deletadas; extração de sistemas de comunicação em nuvem; extração de informações para inferência. Mais informações sobre nossas pesquisas podem ser encontradas em: Iniciativa de Defesa Digital - Data Privacy Brasil.

1.4. Organizações civis como SocialTIC, Red en Defensa de los Derechos Iniciativa de Defesa Digital - Data Privacy Brasil ResearchDigitales (R3D), AccessNow, Amnesty International e CitizenLab desenvolveram metodologias e protocolos para identificar situações nas quais cidadãos, jornalistas e ativistas são alvos de spywares. No Brasil, no entanto, **ainda carecemos de capacidades para realizar esse tipo de análise**, mesmo diante de grandes casos envolvendo spywares, como o caso First Mile (Cognyte).

1.5. O laboratório de detecção de spywares do CitizenLab é uma referência internacional no estudo de tecnologias de vigilância e sua utilização, especialmente no contexto de violações de direitos humanos. Localizado na Munk School of Global Affairs & Public Policy, da Universidade de Toronto, o CitizenLab utiliza uma combinação de metodologias técnicas e investigativas para identificar e analisar spywares, geralmente utilizados por governos e entidades para monitorar dissidentes, jornalistas e ativistas.

1.6. Métodos específicos de análise forense podem incluir a verificação temporal dos eventos observados em logs de sistemas e processos. A correlação temporal é usada para associar a primeira aparição de um item ou processo com a comunicação com servidores conhecidos de ameaças, como o Pegasus, para determinar se um dispositivo foi comprometido. Além disso, a análise pode envolver a revisão de arquivos de banco de dados e *backups* (obtidos por uma extração integral do *filesystem* ou arquivos específicos) para identificar processos ou

atividades associadas a ataques. Essas metodologias ajudam a construir um quadro detalhado das ações dos atacantes e a vincular eventos observados com infraestruturas específicas, como servidores ou redes usadas por grupos de ameaça. Informações detalhadas dessas técnicas podem ser vistas nos relatórios "Forensic Methodology Report: How to catch NSO Group's Pegasus" (2021, Amnesty International) e "New Pegasus Spyware Abuses Identified in Mexico" (2022, CitizenLab).

1.7. Outro aspecto essencial contemplado por este edital é a dimensão psicossocial da violência causada pelo uso de spywares nas vítimas. Propostas que utilizem metodologias humanizadas para abordar essas questões, como a cartilha Guía Contra La Violencia de Género en Línea, produzida pela ONG chilena Amaranta, desempenham um papel crucial na disseminação de conhecimento. Essas iniciativas contribuem para o empoderamento necessário na alfabetização digital e no enfrentamento à violência digital.

2. Escopo do edital

2.1. A Data Privacy Brasil tem investigado e documentado o uso de spywares de forma sistemática no curso do projeto sobre Tecnoautoritarismo nos últimos quatro anos. Casos como First Mile (Abin) são a ponta do *iceberg* de problemas sistêmicos que precisam ser endereçados, incluindo a capacidade de análise forense civil para detecção de *spywares* em dispositivos de cidadãos, como recomendado pelo Comitê de Direitos Humanos do Conselho da Europa.

2.2. A presente convocatória tem o objetivo de **estimular a investigação do uso de spywares em território nacional, contribuindo para o fortalecimento da sociedade civil em mecanismos e protocolos capazes de identificar ameaças de ferramentas de vigilância**. Para isso, serão oferecidas até 3 "financiamentos sementes" para organizações, coletivos ou movimentos sociais que apresentem tanto *iniciativas técnicas*, voltadas para a detecção de spywares e soluções no combate ao uso dessas ferramentas, quanto *iniciativas didáticas*, como a produção de cartilhas educativas, são contempladas por este edital, entre outras propostas considerando os conceitos apresentados nos itens 1.1. e 1.2., bem como a tipologia abrangente de spywares do item 1.3. e os exemplos apresentados nos itens 1.5., 1.6. e 1.7.

2.3. O grupo terá acesso a encontros com o comitê de especialistas na área (Conselho de Especialistas do Programa Malhas Digitais) e com pesquisadores da Data Privacy Brasil com

orientações a respeito das pesquisas realizadas no tema, tipologia e enquadramento jurídico em debate. As organizações selecionadas também farão reuniões remotas, de planejamento e acompanhamento, durante o processo de apuração e elaboração do projeto, em datas a serem combinadas.

3. Sobre o financiamento semente

3.1. O financiamento semente oferecido pela Data Privacy Brasil visa estimular o desenvolvimento de projetos inovadores focados na **detecção e combate ao uso de *spywares* em território nacional**. Ao apoiar três iniciativas de organizações, coletivos ou movimentos sociais, este apoio busca **fortalecer as capacidades da sociedade civil** em lidar com as ameaças de ferramentas de vigilância digital. Com uma estrutura de financiamento inicial, essas organizações terão os recursos necessários para sair do papel e avançar em iniciativas que podem impactar diretamente a proteção de direitos fundamentais no ambiente digital.

3.2. Os projetos apoiados serão incentivados a progredir rapidamente da fase conceitual para a fase de prototipação, com o objetivo de gerar resultados concretos em um período de seis meses. Esse tempo relativamente curto exige que as iniciativas sejam **planejadas de forma ágil e estratégica**, com foco em **metas explícitas e entregas mensuráveis**. O financiamento semente, portanto, não só oferece suporte financeiro inicial, mas também proporciona uma estrutura de acompanhamento técnico e consultivo que maximiza as chances de sucesso e impacto das iniciativas desenvolvidas. Lembrando que é um financiamento semente, portanto, **incentivamos iniciativas gestionárias**, compreendendo o estágio inicial com entregas intermediárias ou prototípicas, mas **com ampla visão e planejamento para frutos e desenvolvimentos futuros**.

3.3. Incentivamos iniciativas criativas no combate aos *spywares*, como soluções técnicas, ferramentas, guias, extensões de navegador, aplicativos, matérias investigativas e jornalísticas, oficinas, entre outros, bem como a combinação de mais de um desses itens. Ressaltamos a importância do apelo social no desenvolvimento dos projetos, estimulando parcerias com movimentos sociais e coletivos.

4. **Condições para submissão de projetos**

4.1. Serão aceitas propostas de **organizações, grupos e coletivos** sem fins lucrativos, mesmo que ainda não formalizadas e/ou que não tenham CNPJ. Também poderão ser aceitas propostas de **empresas de pequeno ou médio porte, microempresas e microempreendedores individuais**, desde que seja justificada a finalidade social da empresa em carta de motivação. Os pagamentos serão efetuados mediante o compartilhamento da respectiva nota fiscal.

4.2. Não serão aceitos projetos apresentados por organizações governamentais, organizações internacionais ou partidos políticos.

4.3. Cada organização, grupo ou coletivo poderá apresentar apenas um projeto. Caso um mesmo grupo ou coletivo envie mais de um projeto, será considerado apenas o último inscrito. Os demais serão desconsiderados.

5. Submissão de propostas

5.1. Os projetos apresentados devem possuir os seguintes elementos básicos:

5.1.1. **Metodologia**: apresente de forma transparente e detalhada a metodologia que será desenvolvida para o projeto piloto de construção de protocolos para detecção de *spywares*. Descreva, por exemplo, se o piloto envolve análise de registros e dados de dispositivos (computadores ou celulares) ou se o piloto envolve outras técnicas de suspeição de ataques (guias sobre tipos mais comuns de ataques via SMS, dicas sobre aquecimento dos dispositivos, ruídos ou indicadores mais comuns.

5.1.2. **Ineditismo ou adaptação**: explique se a metodologia proposta é uma adaptação de abordagens já existentes em centros de pesquisa ou países estrangeiros (práticas já adotadas por laboratórios como Amnesty International ou CitizenLab). Caso afirmativo, detalhe como essas metodologias foram adaptadas para o contexto brasileiro e as modificações feitas para adequar-se às condições locais e necessidades específicas. Descreva de forma objetiva o problema e a solução apresentada em sua proposta.

5.1.3. **Metas e indicadores**: defina as principais metas a serem atingidas no desenvolvimento do projeto piloto. Inclua indicadores claros e específicos que permitirão avaliar o sucesso e o progresso do projeto. Descreva como o piloto será desenvolvido e quais são os critérios para medir seu impacto e eficácia na detecção de spywares.

5.2. As organizações interessadas deverão preencher este formulário até as 23h59 do dia **25 de outubro de 2024** com os seguintes documentos:

5.2.1. **Carta de apresentação** de uma página sobre motivação para submissão de proposta de financiamento.

5.2.2. **Nota conceitual do projeto** contendo, contextualização e objetivo do projeto, os elementos dos itens 5.1.1. (metodologia), 5.1.2 (ineditismo ou adaptação), 5.1.3 (metas e indicadores) e cronograma de execução, **considerando o período de seis meses de execução**.

5.2.3. Orçamento do projeto, em formato simplificado (Excel ou similar), com detalhamento dos custos com pessoas, infraestrutura e gastos operacionais, **com valor máximo de R$50.000,00**.

5.3. A Data Privacy Brasil fará uma reunião online de apresentação e explicação do edital, no dia 08/10/2024, além de outra reunião para tirar possíveis dúvidas, dia 14/10/2024. As informações para participar da reunião estarão disponíveis na página do projeto Iniciativa de Defesa Digital a partir do dia 2/10/2024.

6. Critérios de seleção

6.1. O comitê de avaliação será composto por representantes da Data Privacy Brasil, mais o conselho técnico independente do Malhas Digitais, que analisará e avaliará todas as propostas submetidas.

6.2. Os critérios de avaliação incluem:

(i) **Relevância e impacto social**: A proposta aborda diretamente a questão da detecção e combate ao uso de spywares no Brasil? A iniciativa tem potencial de gerar impacto significativo na proteção de direitos fundamentais e na defesa contra a vigilância digital?

(ii) **Inovação e originalidade**: A proposta apresenta uma solução inovadora ou uma adaptação criativa de metodologias já existentes para o contexto brasileiro? O projeto propõe uma abordagem única para enfrentar desafios locais, como a falta de capacidades forenses cíveis?

(iii) **Metodologia coerente e bem definida**: A proposta contém uma metodologia detalhada e viável para a implementação de protocolos de detecção de spywares? A metodologia técnica ou didática é robusta e adequada ao escopo do projeto?

(iv) **Capacidade técnica e experiência da equipe**: A equipe proponente tem a expertise necessária para desenvolver e implementar o projeto, seja na área técnica ou didática? Existe uma clara demonstração da capacidade técnica da equipe em executar os processos de análise forense, desenvolvimento de ferramentas ou produção de material educativo?

(v) **Viabilidade e execução no tempo proposto**: O projeto é realista em termos de cronograma e pode ser desenvolvido dentro do prazo de seis meses? A proposta possui metas objetivas e indicadores mensuráveis para acompanhar o progresso e o sucesso do projeto?

(vi) **Orçamento adequado e coerente**: O orçamento apresentado é razoável e detalhado, considerando os custos necessários para a execução do projeto? Existe uma boa distribuição dos recursos entre pessoal, infraestrutura e outras despesas operacionais?

(vii) **Colaboração e engajamento com a sociedade civil**: O projeto demonstra envolvimento com movimentos sociais, coletivos ou organizações que trabalham na defesa dos direitos fundamentais? Existe uma estratégia clara de disseminação de conhecimento e fortalecimento da capacidade da sociedade civil para lidar com ameaças de vigilância digital?

7. Das atividades dos selecionados

7.1. As organizações ou coletivos selecionados deverão se comprometer com as seguintes obrigações:

7.1.1. Participar de reuniões quinzenais, com alterações de periodicidade após comum acordo com a Data Privacy Brasil e o Conselho de Especialistas;

7.1.2. Compartilhar as informações sobre o andamento do projeto, em condição de sigilo, com a Data Privacy Brasil e o Conselho de Especialistas, durante a execução do projeto;

7.1.3. Produzir um relatório parcial após três meses de execução do projeto piloto e um relatório final, após a conclusão do período de financiamento (seis meses);

7.2. As entidades selecionadas assinarão um acordo sobre as condições do financiamento semente, com detalhamento das questões de governança, acompanhamento dos projetos e propriedade. O financiamento **não envolverá participação acionária ou qualquer tipo de interferência nos quadros societários ou estatutos das organizações, bem como não implicará em qualquer tipo de relação trabalhista.**

Cronograma

- 04/10/24 a 31/10/24 (23h59): Convocatória
- 08/10/24 às 17h - Live para leitura do edital
- 14/10/24 às 10h - Chamada em vídeo para tirar dúvidas sobre o edital
- 08/11/24: Devolutiva dos projetos selecionados e assinatura do termo de compromisso
- 16/11/24: Início dos projetos e reuniões com os especialistas
- 17/11/24 a 17/05/25: Acompanhamento do desenvolvimento da pesquisa e produção
- 17/02/25: Relatório parcial
- 20/05/25: Relatório e entrega final
- 30/05/25: Evento final

O Programa Malhas Digitais integra o projeto **Iniciativa de Defesa Digital**, organizado em parceria com o InternetLab, e apoiado financeiramente pelo programa ***Spyware Accountability Initiative*** do **New Venture Fund.** Mais informações em: Spyware Accountability Initiative (stopspyware.fund)

Sobre a organização

A Data Privacy Brasil é uma organização que nasce da parceria entre uma escola e uma associação de pesquisa com o objetivo de fomentar a cultura de proteção de dados e direitos digitais no Brasil e no mundo. Para alcançar esse propósito, contamos com o suporte de uma equipe multidisciplinar e oferecemos formações, eventos, certificações, consultorias, conteúdos multimídia, pesquisas de interesse público e auditorias cívicas. Estas iniciativas visam a promover direitos fundamentais e valores ligados à justiça social diante das tecnologias contemporâneas e processos de datificação. Por meio da educação, da sensibilização e da mobilização da sociedade, buscamos uma sociedade democrática na qual as tecnologias estejam a serviço da autonomia, dignidade das pessoas e redução de assimetrias de poder.