INSTITUTO NACIONAL DO SEGURO SOCIAL

Diretoria de Tecnologia da Informação
Coordenação-Geral de Tecnologia da Informação e Segurança
Coordenação de Infraestrutura e Monitoramento de Tecnologia da Informação
Divisão de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos

Relatório

1. A mitigação inicial do evento abarcou as seguintes ações:
- isolamento do ambiente afetado;
- segmentação da aplicação para acesso exclusivo via rede VPN interna e exigência de certificado A3 - Token
- limitação de credenciais autorizadas a acessarem a referida plataforma, com respectivo controle centralizado de autorização de novas credenciais

2. Em 21/05/2024, diante da insistência dos próprios usuários e gestores destes, esta DTIR promoveu o saneamento das credenciais envolvidas e citadas em Relatório da Dataprev como as credenciais que apareceram com o maior volume de tráfego (**Ana Cristina Rodrigues Dutra, Christian da Silva Brito, Omar Gomes de Sena Filho e Paulo Ricardo Brito Cerqueira**). Para esse fim, foram respondidos questionários específicos, e tais usuários orientados a efetuarem as trocas de suas senhas, substituindo-as por senhas de padrão mais seguro.

2. Em 21/05/2024, esta DTIR recebe da Dataprev (CTIR) relação de '*logs*' de acesso do servidor SAMBA , utilizado pela Dataprev para a autenticação no SUIBE, no período do evento (28/03/24 a 07/05/24).

3. Em 22/05/2024, esta DTIR promoveu o saneamento da relação acima, separando as credenciais que tiveram sucesso ('**success**'), das que tiveram alguma falha no acesso ('**fail**'), com planilhas anexadas de números 16602810 e 16602819.

4. Pelo referido relatório da Dataprev (16175919), constata-se que a origem do ataque deu-se por um IP de um servidor NAT utilizado no MDS (Ministério do Desenvolvimento Social), através das credenciais do INSS citadas no item 2.

6. **Esta DTIR esclarece que não houve divulgação, pela Dataprev, e até o presente, de relação de volumetria associada às credenciais envolvidas neste evento.**

7. Foi efetuada uma reunião dia 14/06/2024, entre Dataprev, MDS e INSS, onde os representantes daquele Ministério foram orientados a levantar as localizações efetivas de máquinas do MDS que possam estar associadas a este evento. Até esta data, aguardam-se respostas.

9. Não há portanto, até essa data, elementos para que a resposta à principal questão formulada pela ANPD (volumetria) seja atendida.

Documento assinado eletronicamente por **FRANCISCO HUMBERTO MENDONCA DE ARAUJO**, **Chefe da Divisão de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos** , em 24/06/2024, às 18:52, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.
