Atenção: e-mail enviado para magistrados e servidores sobre contracheques fazia parte de simulação de ataque ao Tribunal

Na simulação realizada entre os dias 12 e 15, um e-mail falso foi enviado para todas as caixas postais da instituição

publicado: **16/09/2022 08h13 última modificação**: **16/09/2022 08h46**

Com o objetivo de mensurar a maturidade dos colaboradores da instituição em relação ao tema Segurança da Informação, a Assessoria de Governança de Segurança da Informação, vinculada à Secretaria de Governança e Gestão Estratégica – SEGGEST, realizou entre os dias 12/09 e 15/09 uma simulação de phishing, mediante autorização da Presidência do Tribunal (PROAD nº 7798/2022).

Em um ataque de mail phishing, e-mail falsos são enviados em nome de uma empresa, serviço ou instituição, solicitando ao destinatário para clicar em um link no texto da mensagem. No entanto, o link não aponta para o que a mensagem oferece, mas sim para um site falso ou arquivo contaminado, visando capturar informações da vítima para utilização em fraudes.

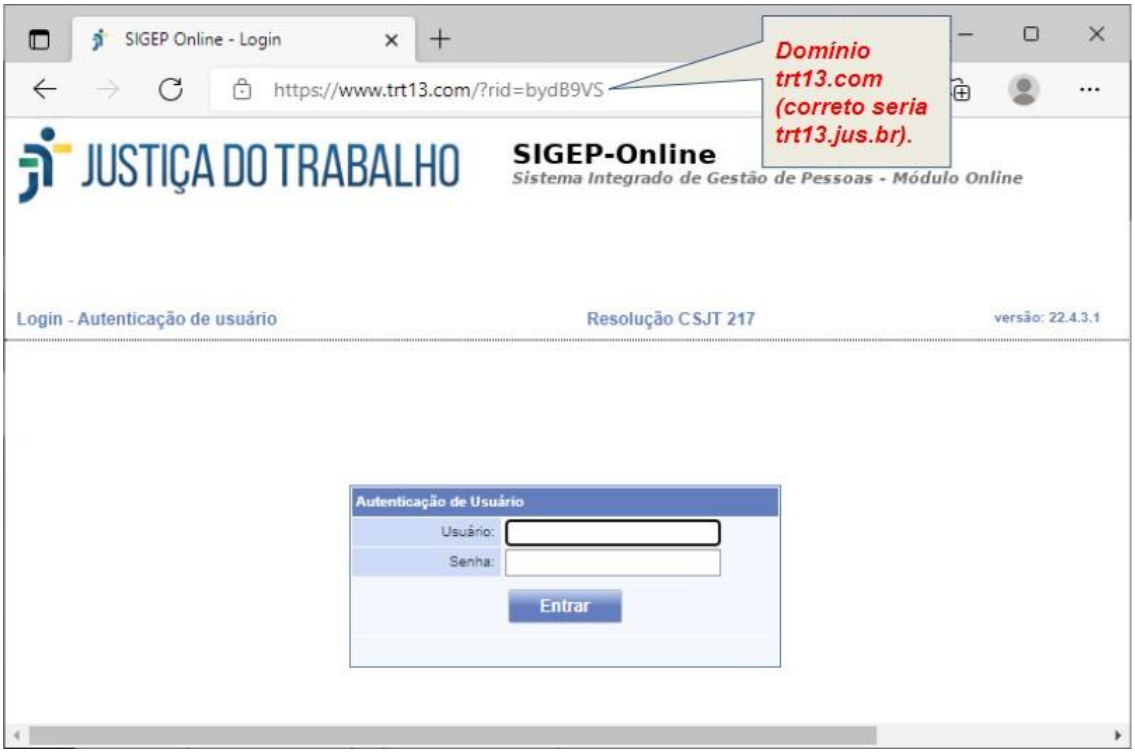
Segundo Rodrigo Mafra, Assessor de Governança de Segurança da Informação da SEGGEST, a maioria dos incidentes cibernéticos ocorridos no Poder Judiciário teve início com o comprometimento de credenciais de acesso (login e senha) de magistrados e servidores, obtidas por meio de phishing, sendo a simulação em questão fundamental para mensurar o nível de exposição da instituição a ataques reais.

Sobre a simulação

Na simulação realizada, um e-mail falso foi enviado para todas as caixas postais da instituição, solicitando aos magistrados e servidores que consultassem seus contracheques clicando no link contido na mensagem, o qual apontava para um site clonado do Sistema Integrado de Gestão de Pessoas – SIGEP.

Segue cópia do e-mail enviado, com alguns indicativos de que se tratava de um e-mail falso:

Site falso do SIGEP, acessado ao clicar no link contido na mensagem:



Resultados da simulação

- E-mail enviado para 1.103 caixas postais;
- 62% abriram o e-mail (691 pessoas);
- 27% clicaram no link (303 pessoas);

- 17% digitaram login e senha (198 pessoas);
- Cabe destacar que na simulação os dados digitados não foram salvos.

Próximos passos

O Secretário de Governança e Gestão Estratégica, Max Frederico, destaca que, a partir da análise dos resultados obtidos, serão propostas ações de capacitação e conscientização em Segurança da Informação para magistrados e servidores, de modo que resultados melhores sejam alcançados em simulações futuras, reduzindo assim os riscos de incidentes cibernéticos causados pelo comprometimento de credenciais de acesso na instituição

Assessoria de Comunicação Social com informações da Seggest

93 visualizações desde a data de publicação