GSI-PR
DEPARTAMENTO DE SEGURANÇA DA INFORMAÇÃO

BIM

Boletim Informativo Mensal

Comunicar para Educar

maio/2022 – Ano 3 – nº 28

Você já imaginou que pode estar colaborando com ataques cibernéticos?

Botnet, cada dia mais sofisticado.

A palavra "***botnet***" é formada pela junção das expressões inglesas ***robot*** (robô) e ***network*** (rede de computadores). O ***botnet*** é um ***malware*** e sua execução ocorre quando uma rede de computadores infectados fica sob o comando de um único computador principal. São geralmente usados para enviar spam, roubar dados pessoais ou executar ataques de DDoS *(Distributed Denial of Service* - Ataque de negação de serviço), que têm como objetivo sobrecarregar um servidor, esgotando os seus recursos e tornando indisponível para os usuários o acesso à rede.

Já o ***bot*** é um tipo de *malware* que permite ao *hacker* obter, de forma remota, o controle completo do computador afetado. Na maioria das vezes, o proprietário do dispositivo nem imagina que está sendo manipulado.

Como esses *bots* são estabelecidos?

O enganador envia campanhas falsas ao usuário por meio de *e-mails*, *SMS* ou anúncios. Com conteúdo bem estruturado e coerente, normalmente ligados à alguma instituição confiável, tais campanhas abordam temas diversos e têm o intuito de, por exemplo, induzir os usuários a concordarem com uma falsa "atualização de informações de segurança de uma conta". Além disso, utilizam a engenharia social (tema já trabalhado em edições anteriores do BIM) para credibilizar as falsas campanhas.

Quais sistemas e dispositivos são os mais vulneráveis?

Os equipamentos mais atingidos são os que possuem tecnologia IoT (*Internet of things* – *internet* das coisas), câmeras, *smartphones*, roteadores e *modems* de banda larga/*Wi-Fi*.

O cibercriminoso utiliza *softwares* sofisticados e medidas cada vez mais eficazes para camuflar o *malware* vetor de ataque e comprometer sistemas e dispositivos. O *malware* precisa ser eficiente, possuir a capacidade de ser imperceptível ao usuário e ser eficaz no momento de sua ativação.

Previna-se!

1. Mantenha atualizados: os *updates* de segurança de seu computador; seus dispositivos *IoT* ; e as versões de *software* dos aplicativos.

2. Dê preferência à instalação de *softwares* originais. Evite instalar aplicativos de desenvolvedores desconhecidos.

3. Utilize um antivírus confiável e o mantenha sempre atualizado.

4. Tome cuidado com *spam, phishing* e outros perigos da *internet*. Evite abrir *e-mails* e *links* desconhecidos.

Como remover o *bot* de uma máquina?

Muitas vezes, o uso de um bom antivírus é suficiente para remover invasões. No entanto, em muitas situações, a remoção só é possível com a formatação do computador ou com a restauração do sistema operacional, e possível retorno aos padrões de fábrica. A dificuldade dependerá do *bot* que infectou o sistema.

Providencie, frequentemente, *backups* de segurança em todos os seus dispositivos. Dessa forma, seus dados estarão protegidos e não serão perdidos em caso de invasão, restauração de sistema ou formatação do dispositivo.

BIM
Boletim Informativo Mensal
Comunicar para Educar
maio/2022 – Ano 3 – nº 28

Você sabia?

Você sabia que o Departamento de Segurança da Informação (DSI/GSI/PR) desenvolveu um **conteúdo programático em segurança cibernética e da informação,** para a capacitação de servidores federais e para subsidiar ações de conscientização da sociedade?

Em 2020, foi estabelecido um grupo de trabalho visando ao cumprimento da competência legal de "**elaborar e implementar programas sobre segurança da informação destinados à conscientização e à capacitação dos servidores públicos federais e da sociedade**", disposta na Política Nacional de Segurança da Informação - PNSI (BRASIL, 2018, art. 12, III). Além da PNSI, conforme a Estrutura Regimental do GSI-PR, publicada em 20 de dezembro de 2019, compete ao DSI "**estimular a formação e a qualificação de recursos humanos na área de segurança da informação**".

O grupo de trabalho organizou os temas a serem abordados em 12 estágios de conhecimento, em ordem de prioridade, dos mais simples para os mais complexos, tendo como resultado o "**Conteúdo Programático em Segurança Cibernética e da Informação",** apresentado por meio da **Nota Técnica nº 11/2021/CGGSI/DSI**.

A Nota Técnica serviu para subsidiar o desenvolvimento da Instrução Normativa de Conscientização, Capacitação e Certificação em Segurança da Informação, que se encontra em fase de consolidação das contribuições recebidas por meio de consulta pública. Além disso, é também referência para os trabalhos desenvolvidos no âmbito do Programa de Acesso Digital (*Digital Access Programme* – parceria estabelecida com o Reino Unido, com vistas a elevar a maturidade da sociedade brasileira nesta temática).

Acesse a Nota Técnica, disponível no site do DSI, e saiba mais! Manter-se informado é manter-se seguro!

CLASSIFICAÇÃO DA INFORMAÇÃO E ATRIBUIÇÃO DE GRAU DE SIGILO

A **Lei de Acesso à Informação – LAI** (Lei nº 12.527, de 18 de novembro de 2011), possui dois preceitos gerais: o da transparência máxima para garantir ao cidadão o direito fundamental de acesso à informação e o do sigilo de certos dados para salvaguardar a sociedade e o Estado.

Isso quer dizer que a informação sigilosa em poder dos órgãos e das entidades públicas, observado o seu teor e em razão de sua imprescindibilidade à segurança da sociedade ou do Estado, poderá ser classificada como RESERVADA, SECRETA OU ULTRASSECRETA.

Por isso, o agente público que decide classificar alguma informação assume grande responsabilidade, pois a atribuição de grau de sigilo, acima ou abaixo do adequado, ocasiona sério prejuízo à administração pública, já que a LAI confere um tempo de restrição para cada grau de sigilo.

Para a correta atribuição do grau de sigilo, é necessário observar o interesse público da informação, devendo ser utilizado o critério menos restritivo possível, levando em consideração a gravidade do risco ou dano à segurança da sociedade e do Estado, bem como o prazo máximo de restrição, ou o evento que defina o final do controle de acesso.

Para saber mais sobre esse assunto acesse o link:
https://www.gov.br/gsi/pt-br/assuntos/dsi/legislacao
http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/decreto/d7724.htm

Fonte: https://www.gov.br/gsi/dsi/ https://www.gov.br/ctir
Editorial/redação/diagramação: AssESI Sugestões: asscom.dsi@presidencia.gov.br