Estratégia

Concursos

Estratégia

Concursos

Segurança da Informação: Golpes e Ataques

ALERJ – FGV – 2017

Ataques cibernéticos podem causar graves prejuízos a pessoas e empresas. Recentemente João recebeu uma mensagem de alerta por e-mail com um pedido para ele atualizar seus dados cadastrais na página do seu Internet Banking.

João não prestou muita atenção em quem enviou a mensagem, nem se era um remetente confiável, e clicou no link presente no corpo do e-mail, que o levou para uma página web, réplica do website real criada por um cyber criminoso.

Como a mensagem de e-mail e o website eram muito bem elaborados, João acreditou estar acessando algo verdadeiro e informou suas credenciais para acesso, quando na verdade ele as entregou a um criminoso.

...

ALERJ – FGV – 2017

...

João foi vítima de um ataque cibernético denominado:

A) DDoS;

B) sniffer;

C) spam;

D) phishing;

E) spoofing.

FBN – FGV – 2013

No que diz respeito aos conceitos na área de proteção e segurança da informação, um termo é utilizado para designar alguns tipos de condutas fraudulentas que são cometidas na rede. É uma espécie de fraude que furta dados de identidade, senha de banco, número de cartão de crédito e informações confidenciais de empresas. O infrator utiliza as informações para fazer saques e movimentações bancárias ou outras operações em nome da vítima.

Assinale a alternativa que indica esse termo.

A) phishing.

B) sniffing.

C) cooking.

D) bullying.

SUDENE PE – FGV – 2013

Um usuário acessa sua caixa de mensagens e abre uma mensagem supostamente enviada pelo seu banco solicitando que ele acesse o site do banco e atualize alguns dados. O usuário clica no link e um site idêntico ao do banco aparece. Ele entra com a sua senha, atualiza os dados e os transmite. Depois de algum tempo, ele percebe que foi enganado, pois uma grande quantia em dinheiro foi retirada da sua conta. Assinale a alternativa que indica o tipo de ataque que ele sofreu.

A) DDoS.
B) phreaking.
C) DoS.
D) phishing.
E) adware.

Câmara de Aracaju - SE – FGV – 2021

O funcionário Fulano da empresa X, cujo e-mail é fulano@empresax.com.br, recebeu um e-mail marcado como importante do Ciclano, do departamento de recursos humanos, com endereço do remetente ciclano@empresax.zhost.ru, contendo em anexo um documento PDF, para ser preenchido até o dia seguinte. Fulano esteve em uma reunião com Ciclano há algumas semanas e acredita que o documento está relacionado com o que foi discutido naquela ocasião. Dados os fatos descritos, Fulano:

A) não deve abrir o documento, pois é uma tentativa de phishing;

B) não deve abrir o documento, pois é um e-mail de spam;

C) deve abrir o documento, pois o antivírus vai emitir um alerta caso seja um vírus;

D) deve abrir o documento, pois um documento PDF não pode conter vírus;

E) não deve abrir o documento, pois o e-mail contém um worm.

AL RO – FGV – 2018

Alguns e-mails se assemelham a outras formas de propaganda, como a carta colocada na caixa de correio, o panfleto recebido na esquina e a ligação telefônica ofertando produtos.

Os e-mails não solicitados, às vezes c
propaganda, que geralmente são enviados pa
um grande número de pessoas são denominac

A) Feed RSS.
B) Tópico.
C) Spam.
D) Assinatura.
E) Threading.

Fonte: CERT.br/NIC.br

IBGE – FGV – 2020

E-mails não solicitados, geralmente enviados para um grande número de pessoas, são rotulados pelo termo:

A) Cookies;
B) Junk;
C) Malware;
D) Phishing;
E) Spam.

SEPOG RO – FGV – 2017

Uma frequente fraude on-line tenta fazer com que os usuários revelem informações pessoais ou financeiras, por meio de uma mensagem de e-mail ou de um sítio web.

Os usuários, em uma mensagem de e-mail, são direcionados para um sítio web que se faz passar por uma entidade de confiança do usuário, em que eles são solicitados a fornecer informações pessoais, como um número de conta ou senha. Essas informações são então utilizadas em roubos de identidade.

Esse tipo de fraude on-line é conhecido como

A) phishing.

B) vírus.

C) criptografia.

D) cavalo de Tróia.

E) spyware.

TJ DFT – FGV - 2022

Marina recebeu uma ligação de um suposto funcionário que dizia estar fazendo uma pesquisa sanitária sobre uma pandemia. Marina passou suas informações pessoais e profissionais, que permitiram ao falso funcionário acessar um sistema com suas credenciais. A técnica empregada pelo falso funcionário para conseguir as informações de Marina é:

A) poisoning;
B) flooding;
C) engenharia social;
D) suborno;
E) sniffer.

BANESTES – FGV - 2021

Antônio recebeu uma mensagem SMS supostamente enviada pela segurança corporativa, orientando-o a clicar em um link para atualizar um cadastro. Ao fazê-lo, Antônio cai em um site falso, mas bastante parecido com o da sua empresa, e fornece dados sigilosos como nome de usuário e senha.

Esse tipo de técnica de engenharia social que se aproveita da confiança depositada por um usuário para roubar dados é denominado:

A) trojan;
B) phishing;
C) spoofing;
D) backdoor;
E) ransomware.

AL RO – FGV – 2018

O tipo de ataque na Internet em que pessoas comuns são contatadas por e-mail, com mensagens que parecem genuínas, contendo nomes e informações que fazem referência a empresas conhecidas, como bancos, porém, contendo links disfarçados para arquivos maliciosos, é denominado

A) Spoofing.
B) DoS.
C) DDoS.
D) Phishing.
E) Bluebugging.

MPE AL – FGV – 2018

Roger é administrador de rede de uma empresa e tem recebido diversas reclamações dos usuários relatando que e-mails aparentemente enviados de uma origem, na verdade, foram enviados de outra. Alguns usuários também reclamaram que, ao navegar para um site, são redirecionados para outro.

A rede que Rogers administra pode ter sido vítima de um ataque que falsifica endereços IP, e-mails e DNS, chamado

A) spoofing.

B) flood.

C) DoS.

D) DDoS.

E) worm.

MPE BA – FGV – 2017

Um cibercriminoso envia para sua vítima um e-mail falso, em que se passa por uma instituição conhecida, informando que seu cadastro está irregular e que, para regularizá-lo, é necessário clicar no link presente no corpo do e-mail.

Esse tipo de falsificação de uma comunicação por e-mail é uma técnica conhecida como:

A) Phishing;
B) Sniffing;
C) MAC Spoof;
D) Denial of Service;
E) SQL Injection.

PREFEITURA DE PAULÍNIA – FGV – 2017

A empresa D2D opera na Internet há três anos. Na semana passada sua página Web foi invadida por hackers que exploraram as vulnerabilidades do servidor Web que estava desatualizado. A página da empresa foi alterada, mas continuou disponível na Internet. O tipo de ataque sofrido pela empresa D2D é conhecido como

A) spoofing.
B) scan.
C) defacement.
D) sniffing.
E) phishing.

DPE RO – FGV – 2015

Uma das formas de ataque à segurança dos dados é o monitoramento de pacotes que passam na rede, procurando por senhas em texto claro, por exemplo. O nome dessa forma de ataque é:

A) Phishing;
B) Scamming;
C) Spoofing;
D) poisoning;
E) sniffing.

IBGE – FGV – 2017

Um dos ataques mais difíceis de combater é o ataque distribuído de negação de serviço (DDoS), em razão da dificuldade de determinar as suas origens.

Uma forma frequente de realizar esse ataque é por meio de:

A) phishing;
B) botnets;
C) ransomware;
D) sniffing;
E) scams.

AL BA – FGV – 2014

Considere que um hacker comprometa milhares de hosts ao redor do mundo, criando uma botnet com intenção maliciosa. Em determinada ocasião, comandados por um computador mestre,estes hosts executam um ataque conjunto a um determinado servidor web ou DNS, consumindo a largura de banda do servidor e comprometendo seu funcionamento.

O cenário descrito é típico de um ataque denominado

A) worms.

B) spoofing.

C) phishing.

D) DDoS

E) DoS.

FIOCRUZ – FGV – 2010

Das alternativas a seguir, assinale a única que contém eventos que caracterizam uma tentativa de ataque do tipo força bruta.

A) A captura de dados sensíveis a partir de um programa espião instalado no computador do usuário.

B) A repetição automática de tentativas de acesso a um recurso protegido, com senhas criadas a partir de combinações aleatórias ou extraídas de listas prédefinidas.

C) A sobrecarga de servidores, alcançada por meio de ataques simultâneos e descentralizados.

D) A operação local e não autorizada de estações ou servidores.

E Brechas resultantes de bugs no sistema.