GAC119 - REO 1: Análises de notícias envolvendo ataques e/ou problemas de segurança

Mateus Carvalho Gonçalves - 201810245
Pedro Antônio de Souza - 201810557

ANÁLISE 1

- **Notícia**

  Site do Ministério da Saúde sofre ataque hacker durante madrugada e sai do ar

- **URL**

  https://www.cnnbrasil.com.br/nacional/site-do-ministerio-da-saude-sofre-ataque-hacker-durante-madrugada-e-sai-do-ar

- **Análise**

  A notícia relata o sequestro dos dados de servidores do Ministério da Saúde. Todos os portais vinculados ao ministério, como o "ConecteSUS" e o "Portal Covid", também foram afetados pelo incidente. O ataque consistiu em intrusão dos servidores e bloqueio dos dados. Segundo o Lapsus$ Group, que assumiu a autoria do ataque, foram copiados 50 TB de dados e, posteriormente, excluídos do sistema do ministério. Como consequência, o acesso ao site oficial da pasta e seus portais foram impossibilitados, caracterizando a negação de serviços (DoS, do inglês Denial of Service). Além disso, o ataque pode ser qualificado como ransomware, já que os responsáveis sugeriram uma negociação para a liberação dos dados.

- **Conceitos importantes de Segurança Computacional na Notícia**

  Negação de Serviços, Intrusão, Ransomware.

ANÁLISE 2

- **Notícia**

  Moradores da 'Cidade do Blockchain' caem em golpe de hacker

- **URL**

  https://www.tecmundo.com.br/mercado/232132-moradores-cidade-blockchain-caem-golpe-hacker.htm

- **Análise**

  A reportagem descreve o roubo das criptomoedas dos cofres de CityDAO, uma organização autônoma descentralizada do estado Wyoming, EUA. Ao adquirir um dos dez mil NFTs emitidos para construção do município, o comprador se torna cidadão de CityDAO e, dentre outros benefícios, garante o direito de acessar o Discord da comunidade. Sabendo disso, um golpista utilizou engenharia social para obter acesso ao Discord de um dos cidadãos e, posteriormente, disparar um ataque de webhook para roubar as reservas da comunidade. A estratégia utilizada pelo cracker foi publicar uma captura de tela falsa em que o primeiro cidadão de CityDAO, denominado Lyons800, alegava estar enganando os demais cidadãos. Através de uma ligação de voz, o golpista persuadiu Lyons800 a deixá-los inspecionar seu console para provar sua inocência e, nesse momento, foi possível obter acesso ao token de autenticação no aplicativo de comunicação. De posse dessa informação, o bandido utilizou funcionalidades oferecidas pelo Discord para iniciar um ataque de webhook.

- **Conceitos importantes de Segurança Computacional na Notícia**

  Phishing, Exploit.

ANÁLISE 3

- **Notícia**

  Sebrae alerta sobre golpes via e-mail e SMS que utilizam seu nome

- **URL**

  https://canaltech.com.br/seguranca/sebrae-alerta-sobre-golpes-via-e-mail-e-sms-que-utilizam-seu-nome-206688/

- **Análise**

  A notícia relata que o Sebrae está alertando a população brasileira de possíveis golpes em nome da companhia que são executados através do envio de e-mail, SMS, WhatsApp ou redes sociais para as vítimas. Os golpistas se passam por funcionários da empresa para oferecer emprego às possíveis vítimas. Assim, atraídas pelos altos salários oferecidos, algumas pessoas informam dados sensíveis aos bandidos para efetivar a contratação. Além disso, há também fraudes utilizando sites falsos com layouts semelhantes ao oficial e envio de e-mails com a promessa de prêmios. Em todos os casos os criminosos se passam pela empresa para capturar dados importantes das vítimas.

- **Conceitos importantes de Segurança Computacional na Notícia**

  Spoofing

ANÁLISE 4

- **Notícia**

  Log4J Vulnerability

- **URL**

  https://blog.gft.com/br/2021/12/23/log4j-vulnerability/

- **Análise**

  A matéria tem como objetivo explicar a vulnerabilidade do framework Apache Log4J 2.x encontrada em dezembro de 2021. A vulnerabilidade ganhou proporções gigantescas pela difusão do uso do software e por ser considerada uma das mais graves já descobertas. Conhecida como Apache Log4j Remote Code Execution (ou CVE-2021-44228), possui a marca de severidade mais alta - 10 em 10. Ela permite que o invasor execute um código arbitrário ao injetar dados em uma mensagem de log. O artigo também aborda temas como os principais frameworks de log para Java e explica questões básicas como por que, o que, quando e onde logar, bem como a manutenção do serviço de logs. Por fim, lista as medidas necessárias caso um projeto tenha a vulnerabilidade.

- **Conceitos importantes de Segurança Computacional na Notícia**

  Exploit, Código malicioso.

ANÁLISE 5

- **Notícia**

  Linux vira alvo de malware na internet das coisas e infecções crescem 35%

- **URL**

  https://tecnoblog.net/noticias/2022/01/18/linux-vira-alvo-de-malware-na-internet-das-coisas-e-infeccoes-crescem-35/

- **Análise**

  A notícia apresenta dados sobre ataques com malware em aparelhos Linux para Internet das Coisas (IoT). Segundo o site, esses ataques cresceram 35% em 2021. Os aparelhos contaminados geralmente são usados para ataques de negação distribuída de serviços (DDoS). As informações foram retiradas da empresa de cibersegurança CrowdStrike, que também lista que as três famílias de malware mais utilizadas foram XorDDoS, Mirai e Moz. A empresa lembra, ainda, que aparelhos de IoT com Linux são extremamente vulneráveis a ameaças, já que os fabricantes nem sempre prestam o suporte necessário, deixando-os com firmware antigos e desatualizados.

- **Conceitos importantes de Segurança Computacional na Notícia**

  Código malicioso (malware), Negação distribuída de serviço (DDoS).