1.Introdução a malwares e seus tipos

Malware é um código ou software projetado especificamente para danificar, interromper, roubar ou geralmente infligir alguma outra ação maliciosa e dispositivos finais são especialmente propensos a ataques de malware. Essa é uma das principais armas dos cibercriminosos. A compreensão dos diferentes tipos de malware é fundamental para a proteção dos sistemas, redes e informações sensíveis.

O ***vetor de ataque*** é o método pelo qual o malware é executado em um computador e potencialmente se espalha para outros hosts da rede. A carga útil (***payload***) é uma ação executada pelo malware que não é simplesmente replicar ou persistir em um host. Exemplos de classificações de carga útil incluem spyware, rootkit, Trojan de acesso remoto (***RAT***) e ransomware.

1.1 Vírus

Um ***vírus*** é um tipo de malware que se espalha inserindo uma cópia de si mesmo em outro programa. Depois que o programa é executado, os vírus se espalham de um computador para o outro. A grande maioria requer ajuda humana para se espalhar e eles podem se instalar na primeira linha de código em um arquivo executável.

Quando ativado, o vírus pode verificar o disco em busca de outros executáveis para que ele possa infectar todos os arquivos que ainda não foram infectados. Eles podem ser inofensivos ou destrutivos, além de serem programados para evitar a detecção. O simples ato de abrir um arquivo pode ativar um vírus. Uma vez ativado, o programa normalmente afetará outros programas no computador ou outros computadores da rede.

1.2 Cavalo de Tróia (*Trojan*)

Um ***cavalo de Tróia*** é um software que parece ser legítimo, mas contém código malicioso que explora os privilégios do usuário que o executa. Muitas vezes são encontrados anexados a jogos on-line, arquivos de música ou até mesmo imagens. Os usuários são comumente induzidos a carregar e executar o cavalo de Tróia em seus sistemas ao jogar o jogo e no fim não notar o problema. O código malicioso continua sendo executado mesmo após o jogo ser fechado. Ele pode causar danos imediatos, fornecer acesso remoto ou receber instruções remotamente para realizar determinadas tarefas.

1.3 Worms

Worms de computadores são semelhantes aos vírus porque se replicam e podem causar o mesmo tipo de dano, porém, eles exploram vulnerabilidades nas redes de forma independente e podem retardá-las à medida que se espalham de sistema para sistema. Enquanto um vírus requer ação humana, worms tem ações independentes e ainda nos dias de hoje representam ameaças persistentes. Geralmente se instalam usando um mecanismo de exploração como um anexo de e-mail, arquivo executável ou cavalo de Tróia. Eles habilitam uma vulnerabilidade, uma maneira de se propagar e todos contêm uma carga (payload).

1.4 Bomba lógica

Uma ***bomba lógica*** é um programa mal-intencionado que pode ser introduzida em um sistema como parte de um programa legítimo, código-fonte ou até mesmo como parte de uma operação criminosa e utiliza um gatilho para ativar código malicioso como datas e horas. A bomba lógica permanece inativa até que o evento acionador aconteça. Assim que ativada, a bomba lógica implementa um código malicioso que danifica um computador. Uma bomba lógica pode sabotar os registros de banco de dados, apagar arquivos e atacar sistemas operacionais ou aplicativos.

1.5 Ransomware

Ransomware é um malware que nega acesso ao sistema de computador infectado ou aos seus dados. Os criminosos cibernéticos exigem então um pagamento para liberar o sistema de computador. Existem dezenas de variantes de ransomware e a maioria dos algoritmos de criptografia utilizados são conhecidos por não serem fáceis de quebrar. Os pagamentos são normalmente pedidos em Bitcoin porque os usuários de Bitcoin podem permanecer anônimos.

1.6 Backdoors

Um ***backdoor*** refere-se ao programa ou código lançado por um criminoso que compromete um sistema. O backdoor ignora a autenticação normal usada para acessar o sistema. Alguns programas comuns de backdoor são o Netbus e Back Orifice, que permitem o acesso remoto a usuários do sistema não autorizado. A finalidade do backdoor é conceder aos criminosos virtuais o acesso futuro ao sistema mesmo se a empresa corrigir a vulnerabilidade original usada para atacar o sistema.

1.7 Spyware

Usado para coletar informações sobre um usuário e enviar as informações para outra entidade sem o consentimento do usuário. Spyware pode ser um monitor de sistema, cavalo de Tróia, Adware, cookies de rastreamento e keyloggers. O spyware pode ser instalado em um sistema por meio de downloads de software, anexos de email, links maliciosos ou explorando vulnerabilidades do sistema; uma vez instalado, o spyware monitora a atividade do usuário, coletando informações sem o conhecimento ou consentimento do usuário; as informações coletadas são geralmente transmitidas para um servidor controlado pelo atacante, onde podem ser usadas para fins maliciosos, como roubo de identidade ou fraude financeira.

1.8 Keyloggers

São um subconjunto de spyware que se concentra em registrar todas as teclas digitadas pelo usuário. Isso inclui senhas, mensagens, detalhes de cartão de crédito e qualquer outra informação digitada no teclado do computador. Esses dados são frequentemente enviados para um servidor controlado pelo invasor. Um keylogger tenta roubar informações confidenciais gravando as teclas digitadas. O invasor geralmente espera descobrir senhas de dados de cartão de crédito.

Keyloggers podem ser instalados da mesma forma que o spyware, frequentemente por meio de downloads de software comprometidos ou anexos de e-mail; uma vez ativados, os keyloggers registram todas as teclas digitadas pelo usuário, incluindo senhas e informações confidenciais; os dados registrados são enviados para um servidor remoto, onde o invasor pode acessar as informações capturadas.

Adware

Exibe pop-ups para gerar receita para o seu autor. O malware pode analisar os interesses do usuário rastreando os sites visitados. Em seguida, ele pode enviar anúncios pop-ups relacionados a esses sites.

1.9 Scareware

Inclui software fraudulento que usa engenharia social para chocar ou induzir ansiedade criando a percepção de uma ameaça. Ele geralmente é direcionado a um usuário desavisado e tenta persuadi-lo a infectar um computador, tomando medidas para resolver a ameaça falsa.

1.10 Phishing

Phishing é um método utilizado em engenharia social envolvendo o envio de mensagens fraudulentas ou a criação de sites falsos. Visa enganar as pessoas e fazê-las divulgar informações confidenciais, como senhas, informações de cartão de crédito, números de seguro social e outros dados pessoais. O phishing pode variar em complexidade, desde ataques simples que visam um grande número de pessoas até ataques altamente direcionados. Para evitar cair em golpes de phishing, é importante que as pessoas estejam cientes das características de mensagens e sites falsos. Elas devem verificar a autenticidade das fontes, não clicar em links suspeitos ou baixar anexos desconhecidos e estar atentas a sinais de alerta, como erros de gramática ou ortografia em mensagens.

- **Mensagem falsa:** O atacante envia mensagens de e-mail, mensagens de texto ou até mesmo mensagens em redes sociais que parecem ser de fontes legítimas. Essas mensagens geralmente alertam a vítima sobre uma suposta situação urgente, como uma conta bloqueada, uma compra não autorizada, ou a necessidade de atualizar informações de login.
- **Isca e página falsa:** A mensagem contém um link ou um botão que leva a uma página falsa que imita um site legítimo, como um banco, uma rede social, ou um serviço de e-mail. Essa página solicita que a vítima insira informações confidenciais, como nome de usuário e senha.
- **Roubo de informações:** Quando a vítima insere suas informações na página falsa, o atacante obtém acesso às credenciais da vítima. Essas informações podem ser usadas para cometer fraudes, acessar contas pessoais ou realizar atividades maliciosas em nome da vítima.

1.11 Spear phishing

O ***spear phishing*** é uma forma mais direcionada de phishing. Nesse caso, os atacantes escolhem alvos específicos, como funcionários de uma empresa, executivos ou indivíduos com acesso a informações sensíveis. Os atacantes coletam informações detalhadas sobre as vítimas, como seus nomes, cargos, interesses, colegas de trabalho e outras informações pessoais. Com base nesses detalhes, eles personalizam mensagens de phishing para parecerem legítimas e confiáveis. Isso aumenta a probabilidade de que as vítimas acreditem nas mensagens e sigam as instruções para divulgar informações confidenciais ou executar ações específicas.

1.12 Vishing

Vishing é o phishing que usa tecnologia de comunicação de voz. Os criminosos podem falsificar as chamadas de origens legítimas usando a tecnologia VoIP. As vítimas também podem receber uma mensagem gravada que pareça legítima, podendo obter números de cartão de crédito ou outras informações para roubar a identidade da vítima.

1.13 Pharming

É a representação de um site legítimo na tentativa de enganar os usuários para inserir as credenciais. O pharming leva os usuários para um site falso que parece ser oficial, então as vítimas digitam as informações pessoais achando que estão conectadas a um site legítimo.

1.14 Smishing

Short Message Service Phishing é o que usa mensagens de texto em celulares. Os criminosos se passam por uma fonte legítima na tentativa de ganhar a confiança da vítima. Quando a vítima visita o site, o malware é instalado no telefone celular.

1.15 Whaling

É um ataque de phishing que busca vítimas de alto perfil em uma empresa, como executivos ou seniores. Outras vítimas incluem políticos ou celebridades. As violações de segurança podem afetar os navegadores da Web, exibindo anúncios de pop-up, coletando informações pessoais identificáveis ou instalando adware, vírus ou spyware. Um criminoso pode invadir um arquivo executável, os componentes ou plugins do navegador. Os atacantes podem se passar por colegas de trabalho, parceiros de negócios ou autoridades para ganhar a confiança do alvo

1.16 Plugins

Os plugins Flash e Shockwave da Adobe permitem a criação de animações gráficas e desenhos interativos que melhoram o visual de uma página da Web. Até pouco tempo, eles tinham um registro de segurança considerável. À medida que o conteúdo baseado em Flash cresceu e se tornou mais popular, os criminosos examinaram os plugins e softwares Flash, determinaram vulnerabilidades e exploram o Flash Player, podendo causar uma falha no sistema ou permitir o controle remoto do sistema afetado.

1.17 SEO poisoning

Os mecanismos de busca como o Google classificam as páginas e apresentam resultados relevantes com base nas consultas de pesquisa dos usuários. Dependendo da relevância do conteúdo do site, ele pode aparecer mais alto ou mais baixo na lista de resultados da pesquisa. SEO é um conjunto de técnicas usadas para melhorar a classificação do site por um mecanismo de pesquisa.

Embora muitas empresas legítimas se especializem na otimização de sites para melhor posicioná-las, o envenenamento SEO usa SEO para que um site mal-intencionado fique mais alto nos resultados da pesquisa. O objetivo mais comum é aumentar o tráfego em sites maliciosos que podem hospedar malware ou executar engenharia social.

1.18 Sequestro de navegador

Um sequestrador de navegador é o malware que altera as configurações do navegador de um computador para redirecionar o usuário para sites pagos pelos clientes de criminosos virtuais. Normalmente, os sequestradores de navegação são instalados sem a permissão do usuário e fazem parte de um download drive-by, que é transferido para o computador automaticamente, quando um usuário visita um site da Web ou visualiza uma mensagem de e-mail HTML.

1.19 Spam

Refere-se ao envio em massa de mensagens não solicitadas, geralmente por e-mail, para um grande número de destinatários. Essas mensagens podem conter anúncios, links maliciosos, conteúdo enganoso ou até mesmo tentativas de phishing. Os spammers enviam grandes volumes de e-mails para endereços de e-mail obtidos de diversas fontes, como listas de e-mails compradas, roubadas ou coletadas na web. O objetivo do spam pode variar, desde promover produtos ou serviços ilegítimos até tentar induzir os destinatários a clicarem em links maliciosos para distribuir malware ou phishing.

1.20 Hoax

É uma mensagem falsa que circula, geralmente pela internet, com informações enganosas ou alarmantes que não são verdadeiras. Hoaxes podem se apresentar como alertas de vírus, histórias sensacionalistas ou teorias da conspiração. Hoaxes geralmente se espalham rapidamente devido à natureza sensacionalista das mensagens. As pessoas são incentivadas a compartilhar essas mensagens com outros, espalhando desinformação. Muitas vezes, hoaxes apelam para o medo, a curiosidade ou a compaixão das pessoas para persuadi-las a agir de acordo com as instruções da mensagem.

1.21 Pretexting

Ocorre quando um invasor chama uma pessoa e mente para ela na tentativa de obter acesso a dados confidenciais.

1.22 Something for something

Ocorre quando um invasor solicita informações pessoais de uma pessoa em troca de algo, como um presente.

1.23 Rootkits

São malwares projetados para se esconder no sistema, tornando-se difíceis de detectar e remover. Eles costumam se enraizar no nível mais profundo do sistema operacional, o kernel, e podem esconder outros tipos de malware. Os rootkits são frequentemente instalados como parte de um ataque de malware mais amplo. Eles ocultam atividades maliciosas, processos e arquivos; os rootkits têm a capacidade de manter-se ativos mesmo após reinicializações do sistema e atualizações de software; a ocultação é usada para esconder a presença de malware no sistema, dificultando a detecção por software de segurança.

1.24 Ataques de dia zero (0day)

Um ataque de dia zero, às vezes chamado de ameaça de dia zero, **é um ataque cibernético que tenta explorar vulnerabilidades de software desconhecidas ou não divulgadas pelo fornecedor de software**. O termo dia zero descreve o momento em que uma ameaça anteriormente desconhecida é identificada. Durante o tempo que os fornecedores de software demoram para desenvolver e liberar um patch, a rede está vulnerável a essas explorações. A defesa contra esses ataques rápidos requer que os profissionais de rede adotem uma visão mais sofisticada da arquitetura da rede. Não é mais possível conter as intrusões em alguns pontos da rede.