1.Outros tipos de malwares

Keyloggers são um dos tipos mais perigosos de malware, pois registram tudo o que o usuário digita no teclado, incluindo senhas, números de cartão de crédito e mensagens privadas. Esse tipo de ameaça é frequentemente utilizado por criminosos para roubar credenciais e obter acesso a contas bancárias, redes sociais e sistemas corporativos. O keylogger permanece residente no sistema e armazena cada pressionamento de tecla em um arquivo, que é posteriormente enviado para os atacantes. Embora medidas como o uso de VPNs e criptografia de dados protejam informações em trânsito, elas não são eficazes contra keyloggers, pois a captura acontece antes mesmo da transmissão dos dados. Além de registrar teclas digitadas, alguns keyloggers avançados também monitoram o conteúdo da área de transferência, tiram capturas de tela e registram conversas de chat, armazenando todas essas informações para posterior envio aos criminosos.

Uma ferramenta popular utilizada para ataques desse tipo é o **DarkComet**, **um trojan de acesso remoto (RAT) que permite capturar não apenas teclas digitadas, mas também capturas de tela e atividades do sistema**. Com esse tipo de software, um atacante pode visualizar em tempo real tudo o que a vítima está digitando, incluindo logins e senhas. O malware registra cada ação do usuário e as armazena em um arquivo que, em intervalos regulares, é enviado para um servidor remoto controlado pelo invasor.

Outro tipo perigoso de malware são as **bombas lógicas (logic bombs)**, **que são programadas para ativar-se em um momento específico ou após a ocorrência de um evento determinado**. Uma bomba lógica pode ser configurada para se ativar em uma data específica ou quando um usuário realiza determinada ação, como fazer login no sistema. Uma vez ativada, ela pode executar comandos maliciosos, como excluir arquivos críticos, corromper dados ou desativar serviços essenciais.

Um exemplo notório de ataque com bomba lógica ocorreu em 2013 na Coreia do Sul, quando um e-mail malicioso foi enviado para bancos e emissoras de televisão. Ao abrir o anexo, um trojan foi instalado no sistema da vítima. No dia 20 de março de 2013, exatamente às 14h, a bomba lógica foi ativada e apagou completamente o conteúdo dos discos rígidos de várias instituições financeiras e empresas de mídia. Os sistemas foram reiniciados, mas como os discos haviam sido apagados, os computadores não puderam mais inicializar, resultando em paralisações massivas. Até mesmo caixas eletrônicos foram afetados, exibindo mensagens de erro ao invés das telas normais de operação.

Identificar bombas lógicas é extremamente difícil, pois elas não possuem assinaturas conhecidas como outros tipos de malware. Como são frequentemente criadas para um ataque específico, não há padrões que possam ser detectados por softwares antivírus convencionais. No entanto, existem medidas preventivas que

podem minimizar os riscos, como a implementação de monitoramento contínuo de arquivos críticos do sistema para detectar alterações suspeitas. Além disso, restringir permissões administrativas apenas aos usuários que realmente precisam reduz a possibilidade de que um atacante instale uma bomba lógica dentro da rede corporativa.

Outro tipo avançado de malware são os **rootkits**, **que se infiltram profundamente no sistema operacional para garantir que permaneçam ocultos**. O nome vem da palavra "root", que em sistemas Unix refere-se ao superusuário, equivalente ao administrador no Windows. O objetivo do rootkit é obter privilégios elevados e esconder sua presença, tornando-se quase invisível para antivírus e ferramentas de segurança.

Rootkits frequentemente se integram ao kernel do sistema operacional, modificando processos internos para evitar detecção. Isso significa que, mesmo que um usuário tente listar os processos ativos no sistema, o rootkit pode alterar essa listagem para esconder sua própria presença. Como esse tipo de malware se torna parte do próprio sistema operacional, removê-lo pode ser extremamente difícil e, em alguns casos, a única solução viável é reinstalar completamente o sistema.

Embora alguns rootkits possam ser detectados por antivírus especializados, a melhor forma de preveni-los é através de medidas como o **Secure Boot**, **um recurso presente na BIOS/UEFI de computadores modernos**. O Secure Boot impede que softwares não autorizados sejam carregados durante a inicialização do sistema, dificultando a instalação de rootkits que tentam modificar o kernel. Dessa forma, mesmo que um rootkit seja instalado, ele será bloqueado antes que consiga afetar o funcionamento do sistema.

2.Keyloggers - Extras

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.

3.Bomba lógica - Extras

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.

4.Rootkit - Extras

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.