DICAS DE SEGURANÇA

Malware - Stealer

Segurança da Informação é responsabilidade de todos!

DICAS DE SEGURANÇA
Malware - STEALER

STEALER o que é?

Stealer é um tipo de malware que tem como objetivo roubar informações sensíveis do usuário, como senhas, cartões de crédito, informações bancárias, histórico de navegação, cookies de websites, capturas de telas, arquivos confidenciais, entre outras. Eles podem ser instalados em dispositivos através de engenharia social, anexos de e-mail maliciosos, downloads de fontes não confiáveis ou através de vulnerabilidades de software. Um dos meios mais comuns de distribuição utilizados pelos malwares do tipo stealer são softwares piratas e portais de download não oficiais, que muitas vezes são impulsionados por anúncios pagos em serviços como o do Google. Os malwares do tipo stealer funcionam de diferentes maneiras, mas geralmente seguem um fluxo de trabalho semelhante ao que segue abaixo:

Fluxo do Malware

Exemplo

1. Instalação: O malware é instalado no dispositivo do usuário através de um dos meios mencionados anteriormente, como phishing, anexos de e-mail maliciosos ou downloads de sites maliciosos.

2. Coleta: Uma vez instalado, o malware começa a rastrear e capturar informações sensíveis, como senhas, números de cartão de crédito e dados bancários. Ele pode fazer isso através da captura de dados digitados pelo usuário, ou acessando arquivos de configuração do sistema.

3. Transmissão: As informações coletadas são então transmitidas aos cibercriminosos responsáveis pela criação do malware, geralmente através da criação de uma conexão remota com um servidor controlado pelos cibercriminosos.

4. Esconder-se: O malware pode se esconder e evitar ser detectado pelos softwares de segurança, a fim de continuar a coletar informações e evitar ser removido do dispositivo.

5. Utilização das informações:
Os cibercriminosos podem usar as informações roubadas para realizar atividades ilícitas, como fazer compras fraudulentas, acessar contas bancárias, ou até mesmo vender as informações para outros cibercriminosos. É importante notar que alguns malwares stealer são mais sofisticados do que outros e podem ter capacidades adicionais, como a capacidade de se espalhar para outros dispositivos, ou a de evitar a detecção pelos softwares de segurança.

Veja algumas dicas de como se prevenir a seguir

PREVENÇÃO - DICAS
Malware - STEALER

Como se proteger?

Existem várias medidas que os usuários podem tomar para se protegerem contra os stealers:

- ❑ Verificar com cautela a legitimidade de portais de download quando desejar que algo seja baixado.
- ❑ Manter o software de segurança atualizado: Um software de segurança atualizado pode ajudar a detectar e remover malwares do tipo stealer.
- ❑ Manter o sistema operacional e programas atualizados é importante para corrigir vulnerabilidades conhecidas que podem ser exploradas por malwares.
- ❑ Evitar clicar em links e anexos desconhecidos: **Não clique em links ou anexos de e-mails ou mensagens de texto desconhecidos**, pois eles podem ser utilizados para instalar o malware no dispositivo.
- ❑ Não utilize softwares piratas ou programas destinados a pirataria, pois além de antiéticos, eles costumam conter programas maliciosos embutidos.
- ❑ Utilizar boas práticas de segurança, como manter senhas fortes, evitar conexões de redes desconhecidas e não compartilhar informações pessoais, pode ajudar a proteger contra ameaças de malware

Segurança da Informação é responsabilidade de todos!