Análise de Malware

Os malwares são artefatos maliciosos que possuem intenção de causar algum tipo de dano a uma máquina ou subtrair algo, na parte de conceitos eu expliquei um pouco melhor sobre malwares e até apresentei para vocês alguns deles, hoje vamos falar um pouco sobre a análise desses artefatos maliciosos.

A análise de artefatos tem diferentes aplicações, pode ser utilizada para ajudar a entender um determinado artefato, seja malware(software malicioso) ou maldoc(documento malicioso) que foi identificado em um incidente, recebido por phishing ou até mesmo enviado por alguém para um grupo de segurança fazer a análise.

O primeiro passo de uma análise é a identificação do artefato, por exemplo, se é um malware ou maldoc, depois de fazer a identificação precisamos entender qual tipo de análise vamos fazer, se vai ser uma análise dinâmica ou estática.

Vamos entender melhor como funcionam essas duas análises:

- **Análise estática**

  A análise estática são os primeiros passos para o estudo de um artefato, é um processo mais manual onde nós observamos o processo de análise de um código ou a estrutura de um programa para determinar sua função. O programa não é executado durante essa análise (dependendo do programa), isso torna o processo dessa análise mais seguro. Na análise estática você pode chegar a algumas conclusões preliminares, mas sempre deve fazer uma análise mais profunda para ter certeza de suas descobertas.

- **Análise dinâmica**

  Esta análise se baseia no comportamento do malware ou maldoc, ou seja, na interação que ele tem quando é executado ou utilizado no caso do maldoc, em outras palavras esta análise é uma análise do artefato em tempo real. Esta análise pode ser facilmente automatizada, existem hoje sites e ferramentas que fazem essa análise de artefatos maliciosos, diferente da análise estática já que depende de um conhecimento técnico por parte do analista ou pesquisador que está fazendo a análise. Essa análise gera uma série de informações que podem ajudar a entender a ameaça cibernética em questão, promovendo a geração de inteligência a partir do comportamento, aumentando a efetividade da detecção.

  Depois de ter se escolhido qual tipo de análise (ou ter feito as duas) é feito um relatório da análise, onde é relatado tudo que foi descoberto e entendido daquele malware, além de como foi feito o processo da análise, após terminar seu relatório você pode partir para tentar desenvolver uma melhoria para prevenir futuras infecções por tal malware, dessa forma você contrói um melhor processo de inteligência cibernética.

jcesar_n

JulioCesarNSM

Obrigado!