FASE DE RECONHECIMENTO

Foto de Noelle Otto no Pexels

Na fase de reconhecimento o atacante procura coletar todo tipo de informação do alvo pretendido. Essa coleta pode se estender além dos meios virtuais indo para a espionagem pessoal, com o uso de engenharia social para se aproximar mais do alvo e observar sua rotina bem de perto. Cyber criminosos podem atuar de várias formas, não duvide da sua capacidade e não ache que ele age somente através de um computador, pois cada etapa do ataque dele, exige uma ferramenta e em alguns momentos a poderosa ferramenta, pode ser uma candidatura a uma vaga de emprego.

Caso seja aceito, ele passa a conhecer por dentro toda a infraestrutura utilizada pela empresa. Já em outros momentos a tão poderosa arma pode ser uma simples conversa, seja ela online ou presencial. Pode ser ainda uma falsa amizade ou um relacionamento, a fim de fisgar e ludibriar um funcionário para que seu ataque seja bem-sucedido.

O objetivo do cyber criminoso é conquistar seu prémio, é ter acesso a rede ou ao sistema do alvo para extrair tudo o que for possível ou o que está previamente planejado.

Dependendo da sua motivação pode ser ainda apagar todos os dados do alvo ou criptografá-los a fim de cobrar pelo seu resgate. Tudo é um passo a passo, em muitos momentos a recompensa ainda é pequena, como pequenas partes de informação

que ele vai cuidadosamente juntando e montando o quebra cabeça, até chegar no nível desejado.

Por isso toda parte de informação é importante, e sabendo disso o atacante vasculha em todos os meios possíveis e imagináveis informações sobre o alvo, e um deles é o próprio site do alvo, onde ele pode obter informações de contato, perfil profissional, parceiros, ramo de atuação, cnpj e se for empresa com ações em bolsa, mais informações públicas destinadas a investidores e por aí vai.

Ele passa um pente fino na vida online do alvo, a fim de obter tudo que pareça relevante e possa ser usado como arma em algum momento.

Essas informações podem servir para forjar um e-mail, com chances de fazer o alvo clicar nele e até se apresentar como um possível parceiro comercial. Por isso a coleta dessas informações por parte do criminoso, acontece ao longo dessa fase de reconhecimento e estudo do alvo, sendo ela de forma passiva ou ativa.

Algumas formas de coleta passiva do alvo são:

- Análise do site da empresa ou pessoal
- Análise nas demais fontes abertas
    - Esta pesquisa em fontes abertas, chamamos de OSINT (Open Source Intelligence). Ela consiste em obter qualquer tipo de informação sobre uma pessoa ou empresa através de diversas ferramentas que a internet nos oferece sem que haja a infração de leis de direitos autorais ou de proteção de dados pessoais, pois afinal de contas, foi o próprio indivíduo quem postou.(tiinside, 2021)
    - O OSINT framework reúne diversas dessas ferramentas categorizadas de acordo com sua finalidade.
        - https://osintframework.com/
- Análise do histórico do site
    - Achive é um site que reúne versões anteriores das páginas web e os atacantes o utilizam em busca de dados sensíveis do alvo.
        - Para isso utiliza-se o site: https://archive.org/
- Análise das redes sociais
- Análise do domínio registrado no Brasil usando whois
    - https://registro.br/tecnologia/ferramentas/whois/
    - Você pode obter o nome do responsável pelo domínio, e-mail de contato, servidores dns usados pelo dono do domínio e etc. Também é possível adquirir serviços de privacidade na compra do seu próprio domínio, caso ele seja adquirido fora do registro.br, porque o registro.br exige a transparência sobre quem é o proprietário do domínio, não possibilitando a privacidade. Um exemplo de serviço de privacidade é o http://www.whoisguard.com/
- Análise de vagas de emprego oferecidas pela empresa para saber quais tecnologias ela utiliza.

ESTE RELATÓRIO AINDA ESTÁ EM ANDAMENTO, SE QUISER DAR SUGESTÕES, ENTRE EM NOSSA COMUNIDADE NO DISCORD: https://discord.gg/N95HY5YSAj

Autor: Felipe Pinheiro

Site: https://backendcore.io

E-mail: contato@backendcore.io

Redes Sociais:

Instagram: https://www.instagram.com/backendcore/

Youtube canal BackEndCore:
https://www.youtube.com/channel/UCNgwVnEvdOvA5hgpajiC_3g

Github: https://github.com/pinheiro-felipe

Facebook: https://www.facebook.com/backendcore

Linkedin: https://www.linkedin.com/in/pinheirofelipe/

Podcast: https://anchor.fm/backendcore

Entre em nossa comunidade backendcore, acompanhe a criação de todos os relatórios e troque ideias. Você é muito bem-vindo(a):
https://discord.gg/N95HY5YSAj