Atualmente os ataques automatizados ocorrem por meio de programas feitos exclusivamente para testar diversos e-mails e senhas no site alvo, dessa forma os atacantes podem apenas deixar o programa ligado em um VPS, com isso o programa irá ficar ligado 24h por dia, 7 dias por semana.

Dentre esses programas, iremos focar no SentryMBA por ser um dos principais e mais famosos softwares utilizados para esse tipo de ataque.

O SentryMBA é um programa gratuito que foi feito para Windows e que por ser extremamente configurável, o torna utilizável para os mais diversos tipos de sites e através desses dois fatores é muito utilizado mesmo após anos de sua criação.

Para abordá-lo, será feita uma análise de seu funcionamento para que toda empresa possa analisar seus métodos de autenticação.

Para começar, vale ressaltar que a base de utilização do programa está em três pilares:

* ComboList: é uma lista que possui e-mails e senhas que geralmente foram geradas a partir de bancos de dados que vazaram de sites, essas listas possuem a senha em texto puro
* Config: é o arquivo de configuração do SentryMBA para um determinado site alvo, ele é gerado e salvo pelo próprio programa em um arquivo .ini, para que esse arquivo seja criado, é necessário analisar os métodos de autenticação no site alvo através de um sniffer juntamente com o SentryMBA para que os parâmetros necessários sejam realizados.
* Proxy: é uma lista de IPs que faz o software ter um IP diferente para cada tentativa de autenticação, a intenção disso é que o sistema de segurança não perceba que o site está sob ataque e assim evitar algum tipo de bloqueio ao IP verdadeiro.

Como demonstração de criação de uma Config para o SentryMBA, iremos utilizar o site X (próprio ou de terceiros?), a primeira etapa afim de obter êxito no ataque é a criação de uma conta comum no site escolhido. Com a utilização de um sniffer iremos fazer a autenticação da conta normalmente com o intuito de entender como o site realiza a checagem de que os dados estão corretos ou não, essa é uma etapa de extrema importância para a configuração, dentro do programa iremos delimitar qual é a palavra-chave que irá identificar o acesso concedido a uma conta e qual irá identificar que os dados estão incorretos.

É nessa identificação que o software separa as contas em que obteve êxito, dessa forma o real atacante pode fazer uso delas.

Ainda na etapa de configuração o atacante pode não querer apenas saber se os dados estão corretos, mas sim buscar mais informações da conta, como se possui algum tipo de saldo, algum cartão de crédito vinculado ou qualquer coisa que seja valiosa para ele e isso também é realizado da mesma forma que mostrada anteriormente, porém nessa etapa não apenas fazemos o SentryMBA entender que ele está no local correto do site, mas agora damos instruções para que ele capture os dados que estão nos campos que delimitamos para ele capturar.