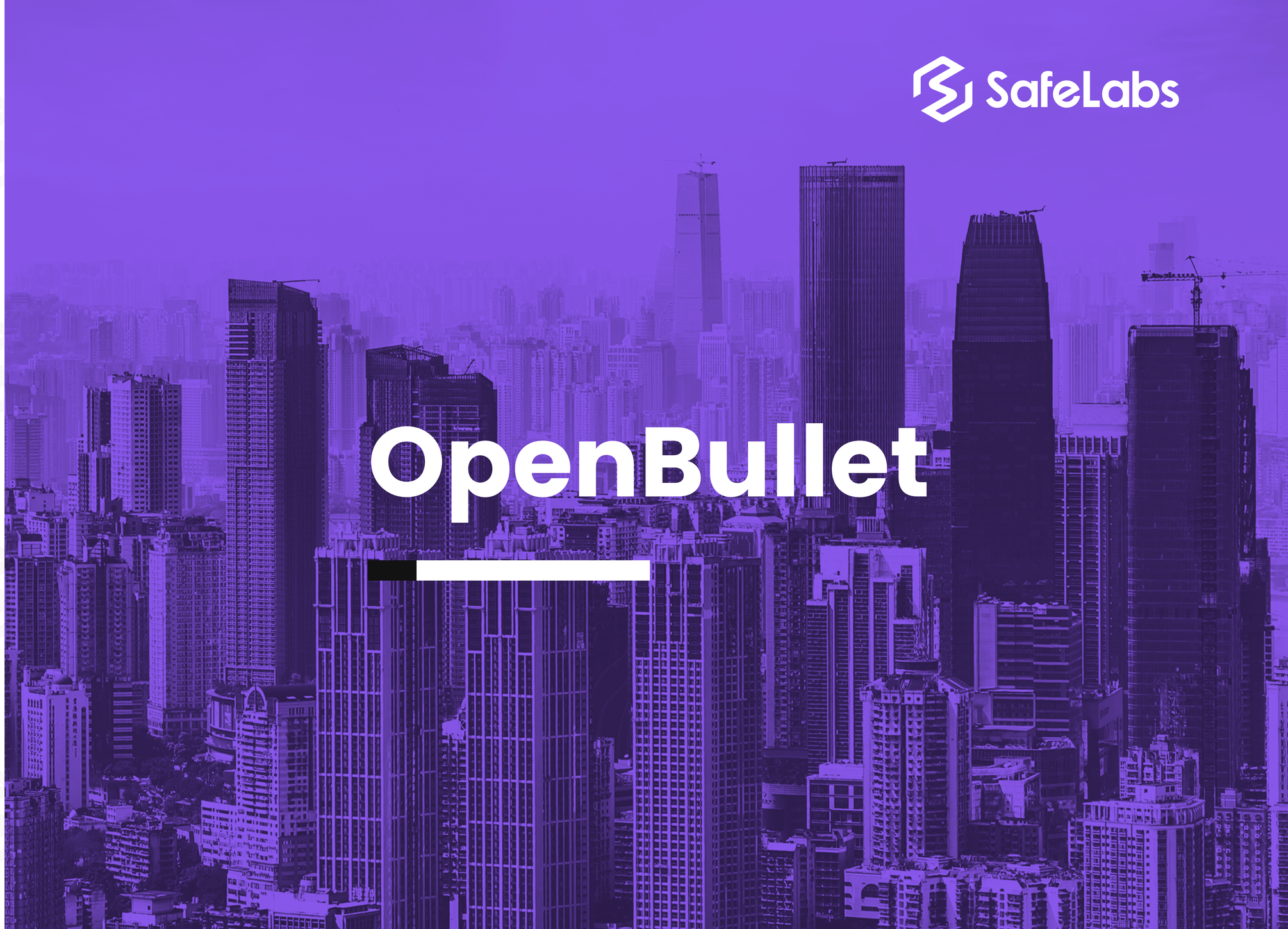
SafeLabs



OpenBullet

OpenBullet

SafeLabs

O OpenBullet é um software legítimo de código aberto para testes de páginas na web, que permite realizar solicitações específicas de coleta de informações. A ferramenta pode ser encontrada no GitHub e pode ser utilizada para diferentes tarefas, como raspagem e análise de dados, pentesting automatizado e testes de unidade usando Selenium – framework utilizado para testar aplicativos web.

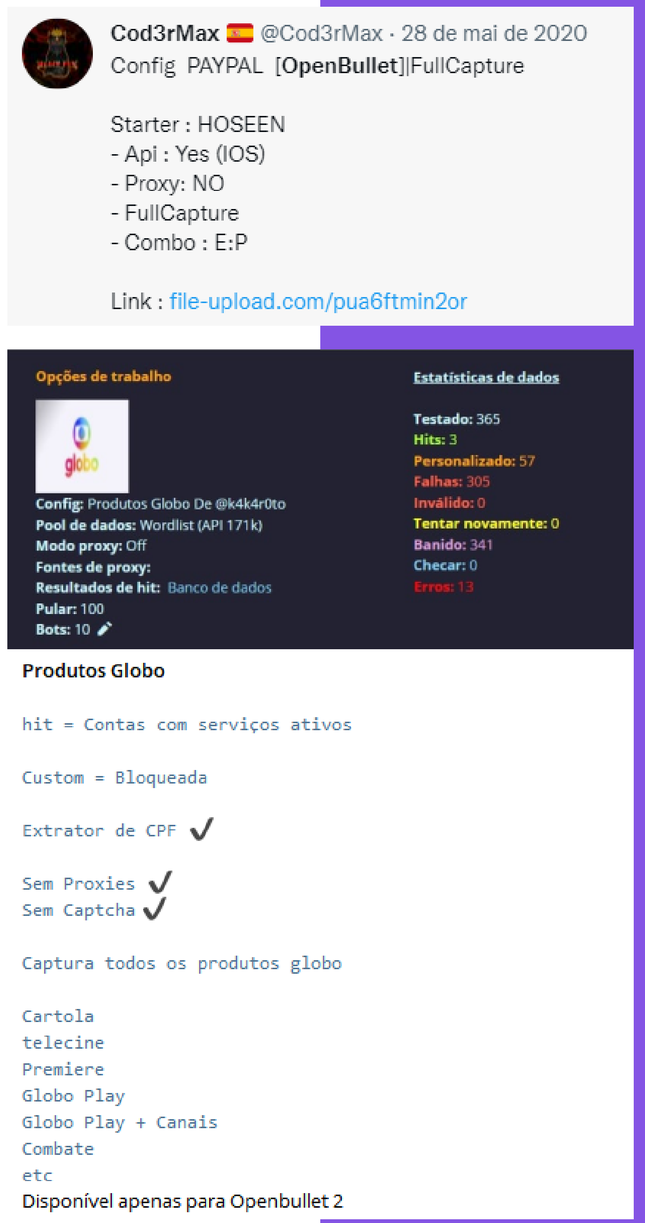
Na sua própria página do GitHub, os criadores informam que o uso não autorizado para preenchimento de credenciais e outros tipos de ataque é ilegal e não se responsabilizam pelo uso indevido, porém o software ganhou notoriedade na comunidade de crimes cibernéticos devido sua natureza de código aberto, permitindo que se personalize os métodos usados pela ferramenta em cada ataque.

Também há outros fatores que atraem os cibercriminosos como à sua manutenção constante e o uso reduzido da unidade de processamento gráfico (GPU) no sistema de destino, tornando-se uma ferramenta muito silenciosa.

Sendo assim, seu código permitiu que desenvolvedores criassem suas próprias versões do software, algumas calibradas para o crime cibernético.

Devido à popularidade do OpenBullet, todo um mercado para scripts de configuração de negociação se formou no submundo, podendo ser encontrados facilmente online, já outras configurações mais confidenciais são vendidas em sites específicos e mercados fraudulentos.

Nas imagens ao lado podemos ver algumas configurações para o software sendo vendidas:



Funcionamento

Os ataques de preenchimento de credenciais incluem as seguintes etapas principais:

1

1. Um invasor obtém credenciais vazadas (ou seja, um par de nome de usuário e senha) de ataques cibernéticos anteriores.

2

2. O invasor usa uma ferramenta de software – OpenBullet – para automatizar o teste de preenchimento dessas credenciais em vários sites e aplicativos móveis.

3

3. Se um conjunto de credenciais for autenticado com êxito, ele será sinalizado como uma conta válida.

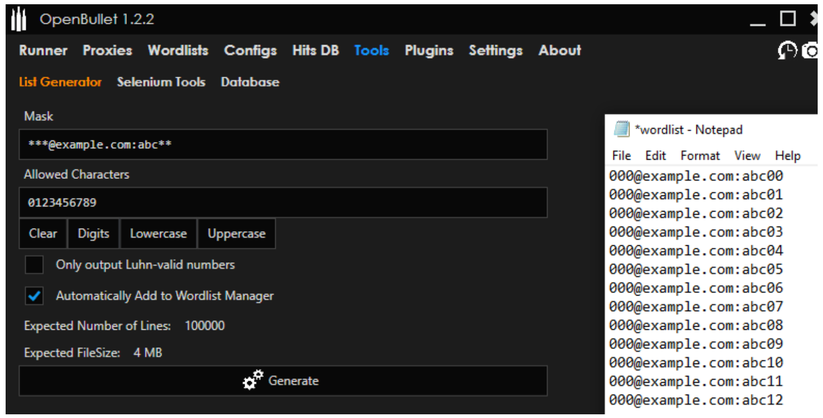
4

4. O invasor agora pode assumir a conta e extrair qualquer valor, incluindo informações de identificação pessoal, informações de cartão de crédito e valor armazenado (como pontos de fidelidade), bem como acessar e-mails, fazer compras fraudulentas e revender a conta.

Alguns recursos do OpenBullet utilizados ilicitamente

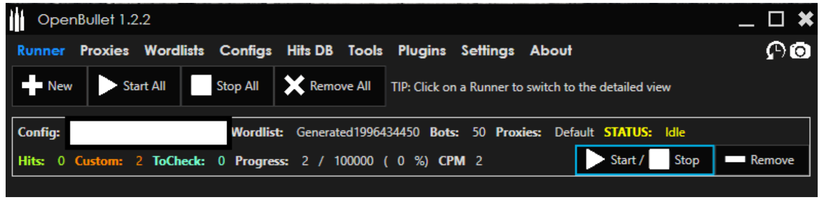
1. List Generator

Essa guia permite que o usuário importe milhares de palavras que podem ser usadas ao tentar se conectar a sites segmentados. Uma entrada pode ser tão simples como “endereço de e-mail: senha” ou “login:senha ”.



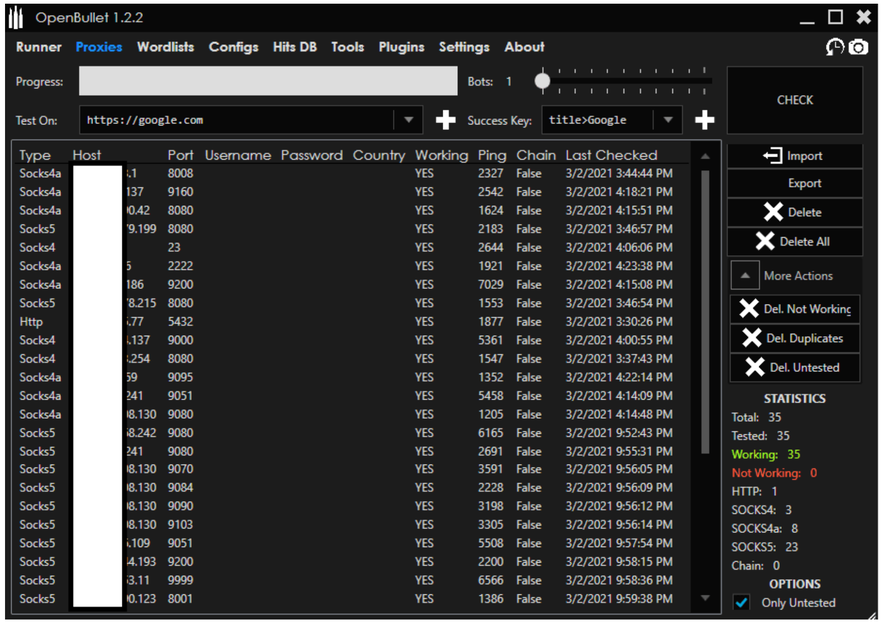
2. Runner

Um usuário pode selecionar essa guia para iniciar um ataque de credencial usando o OpenBullet. A guia do corredor mostra o progresso e o número de acessos positivos para cada site que está sendo testado.



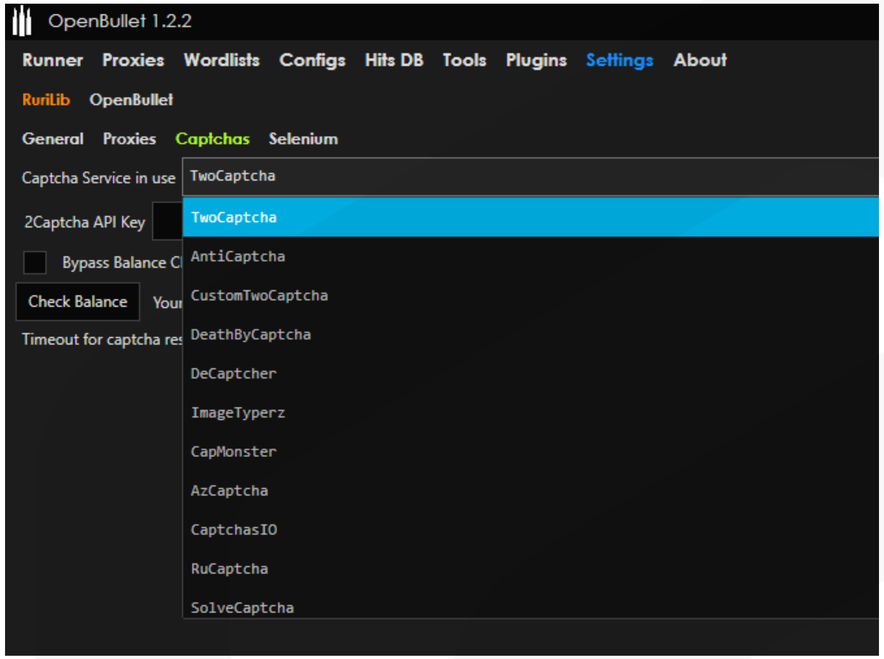
3. Proxies

Os proxies são uma parte importante do OpenBullet. Eles permitem aos usuários várias tentativas de login usando um endereço IP diferente para cada tentativa. Além disso, eles podem configurar o tempo entre cada tentativa de conexão, para que cada tentativa não gere nenhum alarme no site de destino para uma atividade de login incomum que normalmente seria gerada por um grande número de tentativas em um período muito curto.



4. Ferramentas, plug-ins e configurações

Os plug-ins podem ser facilmente importados para o OpenBullet para diferentes propósitos. As possibilidades são aparentemente infinitas, desde que a finalidade do usuário envolva enviar e coletar dados para um site direcionado. Na guia de configurações, os usuários do OpenBullet podem ajustar as configurações do sistema, como ignorar CAPTCHAs, por exemplo.



Maneiras de se proteger contra-ataques de preenchimento de credenciais

1. **Boas práticas na criação de senhas.** Os usuários devem evitar usar senhas fracas, enquanto as organizações devem implementar uma lista de bloqueio de senhas comumente usadas para impedir que os usuários as criem. Os usuários também devem evitar a reutilização de credenciais para várias contas e serviços online.

2. **Habilite a autenticação multifator – MFA em sites e serviços.**

3. **Crie um PIN ou responda a perguntas de segurança adicionais.** Alguns sites permitem que os usuários respondam a perguntas de segurança adicionais ou forneçam um PIN exclusivo para autenticação adicional.

4. **Habilite a análise de tentativas de login.** Alguns sites e serviços, como provedores de serviços de e-mail, executam análises de tentativas de login. Estes são baseados em diferentes fatores, incluindo:
   - **I.** Informações do navegador. Uma tentativa de login com um navegador diferente, que nunca foi escolhido por um usuário, pode indicar uma tentativa de login fraudulenta.
   - **II.** Endereço IP. Os usuários que alteram repentinamente o endereço IP e/ou o país de origem podem ser um bom indicador de tentativa fraudulenta.


SafeLabs