Identificação de cryptojacking: Uma Análise de ferramentas

Isadora Barroso Passos
Bacharelado em Sistemas de Informação - Centro Federal de Educação Tecnológica Celso Suckow da Fonseca (Cefet-RJ)
Nova Friburgo, Brasil
isadora.passos@aluno.cefet-rj.br

Gabriel Pinto de Souza
Bacharelado em Sistemas de Informação - Centro Federal de Educação Tecnológica Celso Suckow da Fonseca (Cefet-RJ)
Nova Friburgo, Brasil
gabriel.pinto@aluno.cefet-rj.br

Nilson Mori Lazarin
Bacharelado em Sistemas de Informação - Centro Federal de Educação Tecnológica Celso Suckow da Fonseca (Cefet-RJ)
Nova Friburgo, Brasil
nilson.lazarin@cefet-rj.br

ABSTRACT

This study explores the surge in cryptojacking due to the widespread popularity of cryptocurrencies. With a focus on safeguarding users against unauthorized cryptocurrency mining, the article evaluates five browser extension. Moreover, was developed a bot that can analyze infected sites, generating a final list that was then tested with the extensions to compare their performance. Additionally, the study produces an updated list of infected sites by processing URLs from two distinct databases. The bots enable testing with different databases, facilitating the assessment of various protection tools against cryptojacking.

KEYWORDS

Cryptojacking, Tools, Cybersecurity

1 INTRODUÇÃO

Uma criptomoeda é um ativo digital registrado em blockchain, que usa criptografia para garantir a rastreabilidade e integridade das transações. Diferente de moedas convencionais, estas não possuem uma autoridade central que as emite ou regula, ao invés disso utilizam um sistema distribuído que permite registrar transações e a emissão. Além disso, essa tecnologia tem gerado muito interesse por conta do alto lucro proveniente de sua valorização [1].

A mineração de criptomoedas é o processo pelo qual novas unidades são emitidas. Este processo envolve a resolução de complexos problemas matemáticos usando poderosos computadores. Os mineradores competem para resolver esses problemas e, quando conseguem, são recompensados com novas unidades da criptomoeda e com as taxas de transação associadas a geração de novos blocos na rede. Isso incentiva os mineradores a dedicarem seu poder computacional para manter a segurança e a integridade da rede [2].

Nos últimos anos, a mineração de criptomoedas tornou-se uma atividade muito lucrativa. Isso acabou atraindo cibercriminosos que passaram a praticar *criptojacking*, o roubo do poder computacional para mineração de criptomoedas [3, 4]. Este tipo de ataque tem ocorrido de várias formas, desde a criação de *forks* infectados de projetos populares em plataformas Git, a inclusão de softwares maliciosos em lojas de aplicativos móveis, a disponibilização de imagens de contêiner infectadas, ou ainda, através da injeção de scripts maliciosos em sites, de forma que, quando visitadas, exploram o poder de processamento do lado do cliente [5, 6].

Este trabalho apresenta um levantamento e um comparativo de ferramentas capazes de proteger o lado cliente, no caso de acesso a uma página web infectada com *criptojacking*. Neste estudo, foi definida uma métrica para a análise das ferramentas: a eficiência, com foco na proteção do usuário. Essa métrica abrange a capacidade das ferramentas em identificar com precisão scripts de mineração não autorizados, bem como a eficácia em bloquear ativamente esses scripts. Essa eficácia desempenha um papel crucial na prevenção de impactos negativos nos usuários, assegurando a proteção de seus recursos de computação e reforçando a segurança contra atividades indesejadas e potencialmente prejudiciais.

2 TRABALHOS RELACIONADOS

O trabalho de Tekiner et. al, 2021 [7] destaca o *cryptojacking* como uma ferramenta fundamental para atacantes, impactando várias áreas, desde instituições financeiras até plataformas de vídeo e videoconferência. O artigo reconhece limitações nos métodos de detecção existentes, destacando a capacidade dos atacantes de contorná-los. Para abordar esse problema, ele propõe uma análise sistemática do malware, baseando-se em pesquisas acadêmicas, conjuntos de dados e casos de ataques, além de fornecer insights e direções de pesquisa para a comunidade acadêmica interessada nesse tópico emergente.

O artigo de Saad et. al, 2018 [8] destaca o rápido crescimento do *cryptojacking*, que teve um aumento de 8500% em 2017. Os autores conduzem uma análise abrangente, tanto de forma estática quanto dinâmica. O artigo também revisa as contramedidas existentes e suas limitações, e sugere contramedidas de longo prazo com base nas análises realizadas.

O trabalho de Carvalho e Lazarin, 2023 [9] apresenta a criação de uma extensão de navegador que compara os dados do domínio com os dados administrativos advindos da ReceitaWS, uma empresa que fornece uma API gratuita para obtenção de dados de pessoas jurídicas, as informações são pegas diretamente da Receita Federal. Caso a comparação indique inconsistência nos dados é gerado então um aviso para o usuário, que tomara a decisão de sair ou prosseguir no site, evitando assim que pessoas maliciosas repliquem páginas famosas com o intuito de roubar dados e capacidade de processamento do dispositivo dos usuários.

Este trabalho busca expandir essas pesquisas, ao focar a avaliação de ferramentas destinadas à proteção contra mineração não autorizada, do lado do cliente. Além disso, apresentamos uma abordagem prática ao testar essas ferramentas em uma base de dados conhecida de sites infectados, proporcionando uma análise comparativa de eficácia. Buscando, dessa forma, fornecer insights sobre a aplicabilidade e eficiência prática dessas ferramentas em cenários específicos de detecção de cryptojacking.

3 METODOLOGIA

Este trabalho se concentra na análise de desempenho de ferramentas de proteção do lado cliente. Essas foram submetidas a uma lista de sites infectados por *cryptojacking*, permitindo uma avaliação da detecção e bloqueio desse malware em um cenário real.

Buscando avaliar as ferramentas, adotamos uma abordagem de seleção de extensões para o Google Chrome, escolhido por ser o navegador mais utilizado em 2023 [10]. O processo de seleção seguiu duas etapas: Inicialmente, realizamos uma pesquisa com a palavra-chave "*cryptojacking*", na loja de extensões do Chrome, buscando identificar as extensões disponíveis. Nesta etapa obtivemos uma lista com 10 resultados. Em seguida, utilizamos um critério de classificação baseado na descrição da extensão ter especificado a realização do bloqueio contra cryptojacking. Com base nesses critérios, selecionamos as cinco primeiras extensões disponíveis, que foram:

- *Easy Redirect && prevent Cryptojacking*[1] (Versão 3.7.0): bloqueia URLs prejudiciais e redireciona o usuário através do uso de expressões regulares, protegendo-o contra a criptomineração;
- *Bloqueador de anúncio do AdGuard* [2] (Versão 4.3.12): bloqueia anúncios do Youtube e do Facebook, em sua descrição também é mencionada a proteção contra instaladores de adware, spyware, malware, phishing e cryptojacking;
- *CoinEater*[3] (Versão 0.1.3): bloqueia mineradores de criptomoedas como o CoinHive, sua lista de bloqueio é baseada em verificações regulares da internet, dentro de um projeto de pesquisa científica feito pelo Instituto de Pesquisa em Segurança de TI da Universidade de Ciências Aplicadas de St. Pölten;
- *minerBlock*[4] (Versão 1.2.18): extensão de navegador que visa bloquear mineradores de criptomoedas baseados em navegador em toda a web. A extensão usa duas abordagens diferentes para bloquear mineradores. O primeiro é baseado no bloqueio de solicitações/scripts carregados de uma lista negra, esta é a abordagem tradicional adotada pela maioria dos bloqueadores de anúncios e outros bloqueadores de mineração. A outra abordagem detecta o comportamento potencial de mineração dentro de scripts carregados e eliminá-os imediatamente;
- *Miners Shield*[5] (Versão 0.1.6): Utiliza os dados de consumo da CPU do usuário para prevenir de possíveis ataques de criptojacking, bloqueando os sites responsáveis pelo aumento da utilização.

Para a realização deste trabalho utilizou-se quatro máquinas virtuais distintas, com o sistema operacional Ubuntu recém instalado, a fim de evitar que fatores externos impactassem o resultado do trabalho. O BOT foi configurado para baixar a extensão no momento da execução, garantindo a precisão dos testes individuais de cada uma delas. Além disso, o BOT foi programado para verificar a presença da mensagem de bloqueio padrão na tela ao acessar uma URL, uma vez que o foco principal do estudo era avaliar as listas de bloqueio de cada ferramenta. No entanto, é possível ajustar facilmente o BOT para outras abordagens, como verificar a capacidade de bloqueio das extensões em tempo real, o que pode ser útil para pesquisas futuras.

3.1 Defnição da amostra

Para conduzir o experimento com as extensões selecionadas, foram utilizadas duas bases de dados distintas. A primeira base consistia em 3496 endereços de URLs[6], e a segunda possuía 490 URLs[7], elas foram então combinadas em uma única base de dados, possuindo 3986 URLs no total.

Posteriormente, desenvolvemos um BOT capaz de inserir os endereços da base de dados resultante da primeira fase no navegador e verificar a resposta do servidor. Caso o servidor respondesse com *status* 200, indicando que o site estava ativo e funcionando, o BOT então classificava o site como acessível, das 3986 URLs processadas 573 estavam ativas.

Por fim, utilizamos a ferramenta Dr.Mine[8] (um script Node que identifica automaticamente as requisições de criptomineradores online) para validar quais URLs estavam efetivamente infectadas. O arquivo com os sites infectados foi percorrido com um BOT cuja função era fazer a remoção de possíveis URLs repetidas, bem como separar cada linha do arquivo com um único endereço de URL, após a limpeza foram identificadas 384 sites únicos infectados.

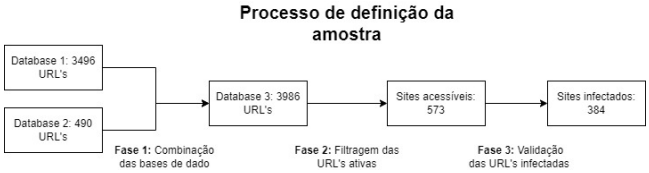

Figure 1: Descrição do processo de definição da amostra.

3.2 Análise das ferramentas

Para verificar a quantidade de sites bloqueados por cada extensão, foi criado um teste automatizado para percorrer cada site da lista e verificar se uma mensagem de bloqueio era exibida. A execução foi acompanhada para os primeiros 30 sites, em cada extensão, a fim de verificar se o mesmo estava funcionando corretamente e se a extensão estava devidamente configurada. Ao final do processo, os sites bloqueados foram contabilizados e as URLs correspondentes foram registradas.

Os resultados são apresentados na Tabela 1 e o Figura 2. A extensão *Miner Block* obteve o melhor desempenho 27.08%, conseguindo bloquear 104 dos 384 sites infectados com *cryptojacking*, seguida da extensão *Easy Redirect* com 1.56% e da extensão *Miners Shield*

[1] https://chromewebstore.google.com/detail/easy-redirect-prevent-cry/kceciaijnoaceceljkggfocngjleimem
[2] https://chromewebstore.google.com/detail/bloqueador-de-an%C3%BAncio-do/bgnkhhnnamicmpeenaelnjfhikgbkllg
[3] https://chromewebstore.google.com/detail/coineater/mphghokdjcoojfjbmldmjodgmbjchnlp
[4] https://chromewebstore.google.com/detail/minerblock/emikbbbebcdfohonlaifafnoanocnebl
[5] https://chromewebstore.google.com/detail/miners-shield/kenkfifencmkppalflbkaiigbkgljkno
[6] https://gitlab.com/ZeroDot1/CoinBlockerLists/-/tree/master
[7] https://github.com/mmg1/blocklists/tree/master
[8] https://github.com/1lastBr3ath/drmine

com 1.30% de taxa de acerto. As extensões *Bloqueador de anúncio do AdGuard* e *Coin Eater* não foram capazes de bloquear o acesso a sites infectados.

Extensões	Quantidade de usuários	Quantidade de sites bloqueados
Miner Block	200.000	104
Bloqueador de anúncio do AdGuard	13.000.000	0
Easy Redirect	2.000	6
Coin Eater	893	0
Miners Shield	104	5

Table 1: Sites bloqueados por cada ferramenta.

Buscando garantir a reprodutibilidade do experimento realizado, todos os arquivos e bots desenvolvidos estão disponíveis para download[9].

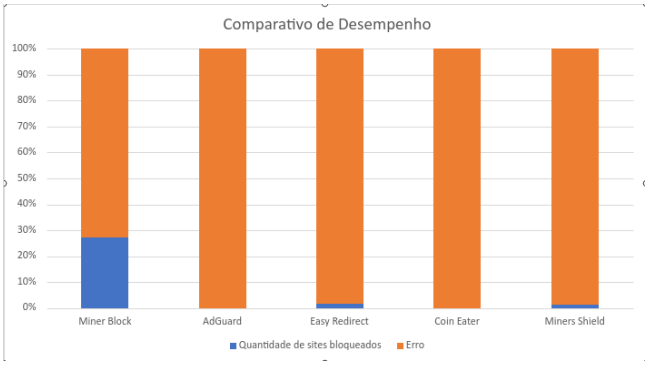

Figure 2: Comparativo de desempenho.

4 CONSIDERAÇÕES FINAIS

Este trabalho apresentou um comparativo entre as extensões de proteção contra *cryptojacking* mais populares, disponíveis para o navegador de internet mais utilizado no mundo e os resultados obtidos são alarmantes, pois o melhor desempenho apresentado, da extensão Miner Block, é menor que 30%. Além disso, o Bloqueador de anúncio do AdGuard tinha a maior quantidade de usuários entre as extensões testadas e apresentou um dos piores resultados, não sendo capaz de identificar e bloquear nenhum dos sites infectados.

É importante ressaltar que os resultados apresentados podem ser influenciados pela escolha das bases de dados utilizadas, dados obtidos podem variar em futuras execuções dos *bots*, por conta de mudanças nas disponibilidades dos sites e de atualizações das ferramentas. As discrepâncias nos números de bloqueios podem ser atribuídas às características específicas de detecção de cada extensão, bem como à natureza dinâmica das ameaças de *cryptojacking*.

Dessa forma, trabalhos futuros podem analisar outras ferramentas, tais como antivírus ou firewalls, ou ainda, propor uma extensão para navegador, na tentativa de obter melhores resultados. Além disso, novas bases URLs infectadas poderão ser utilizadas.

[9] https://github.com/LabRedesCefetNF/Passos_2023_CryptojackingToolAnalyzer

REFERENCES

[1] kaspersky. O que é criptomoeda e como funciona?, May 2023. URL https://www.kaspersky.com.br/resource-center/definitions/what-is-cryptocurrency.

[2] Pedro Ramos Brandão. Criptomoeda: o Bitcoin. *Revista de Ciências da Computação*, pages 1–20 Páginas, December 2020. doi: 10.34627/RCC.V15I0.258.

[3] Jérôme Segura. The state of malicious cryptomining | Malwarebytes Labs, February 2018. URL https://www.malwarebytes.com/blog/news/2018/02/state-malicious-cryptomining.

[4] Cryptocurrency. Cryptocurrency, September 2023. URL https://en.wikipedia.org/w/index.php?title=Cryptocurrency&oldid=1173772966. Page Version ID: 1173772966.

[5] Saide Manuel Saide, Ednilson Luis Alfredo Sarmento, and Felermino D. M. A. Ali. Cryptojacking Malware Detection in Docker Images Using Supervised Machine Learning. *International Conference on Intelligent and Innovative Computing Applications*, 2022:49–56, 2022. URL https://doi.org/10.59200/ICONIC.2022.006.

[6] Nada Lachtar, Abdulrahman Abu Elkhail, Anys Bacha, and Hafiz Malik. A cross-stack approach towards defending against cryptojacking. *IEEE Computer Architecture Letters*, 19(2):126–129, 2020. URL https://doi.org/10.1109/LCA.2020.3017457.

[7] Ege Tekiner, Abbas Acar, A. Selcuk Uluagac, Engin Kirda, and Ali Aydin Selcuk. Sok: Cryptojacking malware. In *2021 IEEE European Symposium on Security and Privacy (EuroSP)*, pages 120–139, 2021. URL https://doi.org/10.1109/EuroSP51992.2021.00019.

[8] Muhammad Saad, Aminollah Khormali, and Aziz Mohaisen. End-to-End Analysis of In-Browser Cryptojacking, September 2018. URL http://arxiv.org/abs/1809.02152.

[9] Brayner Carvalho and Nilson Lazarin. Análise de dados administrativos de e-commerce: Uma abordagem focada no cliente. In *Anais Estendidos do XXIII Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais*, pages 243–248, Porto Alegre, RS, Brasil, 2023. SBC. URL https://doi.org/10.5753/sbseg_estendido.2023.233492.

[10] Browser Statistics. URL https://www.w3schools.com/browsers/.