TÉCNICO LISBOA

Identificação e Análise de *Cryptojacking*:
Efeitos no desempenho

João Manuel Roxo Carreiro

Tese para obtenção do Grau Científico de Mestrado em

Segurança de Informação e Direito no Ciberespaço

Orientador: Prof. Dr. Miguel Nuno Dias Alves Pupo Correia

Júri

Presidente: Prof. Dr. Paulo Alexandre Carreira Mateus
Orientador: Prof. Dr. Miguel Nuno Dias Alves Pupo Correia
Arguente: Prof. Dr. Nuno Miguel Carvalho dos Santos

Outubro de 2019

Agradecimentos

Expresso a minha gratidão a todos os que, de alguma forma e em algum momento, direta ou indiretamente, contribuíram para este estudo. Para o efeito, surge a necessidade de manifestar, em especial, o meu agradecimento:

Ao orientador, Professor Doutor Miguel Correia, do Instituto Superior Técnico de Lisboa, pela disponibilidade constante, por toda a atenção dispensada, pela paciência, dedicação e pelo elevado profissionalismo.

A todos os meus familiares e amigos que me apoiaram neste percurso e que se predispuseram a auxiliar e rever o trabalho, ao longo do tempo.

Bem-haja a todos.

Resumo

A evolução tecnológica, associada a novas metodologias e procedimentos para resolução dos problemas humanos, é, por norma, seguida pelo desenvolvimento nas atividades criminais. O surgimento da *blockchain* e de criptomoedas confere distintas possibilidades para a realização de pagamentos, anonimização de processos e investimentos, ao mesmo tempo que se materializa numa nova oportunidade para agentes mal-intencionados gerarem formas ilícitas de obtenção de rendimento.

Um dos resultados desta normalização é o *cryptojacking*, que integra a categoria dos *malwares* lucrativos e se traduz na introdução de códigos maliciosos em programas locais ou em sites online, com o fim de desviar capacidade de processamento dos dispositivos afetados para mineração não consentida de criptomoedas. Pela primeira vez na história, as incidências deste tipo de *malware* ultrapassaram as de *ransomware*, tornando relevante o estudo do fenómeno, a compreensão da problemática e a análise das suas caraterísticas.

Nesse sentido, o presente trabalho consiste em enquadrar devidamente este *malware* no quadro teórico, complementando-se por uma parte prática em que se executaram experiências, em ambiente controlado, com diferentes variáveis e propriedades, para analisar e aferir os efeitos do *cryptojacking* no desempenho de um sistema computacional.

Conclui-se que há vários tipos de *scripts* para mineração ilícita de criptomoedas em sites, que é possível presumir a existência de *cryptojacking* pela análise de desempenho do sistema afetado, que há relação direta entre a percentagem de utilização da CPU e a ativação do *malware*, e que a temperatura registada após cada teste também é indicadora dessa atividade.

Palavras-chave: Criptomoedas, *Malware*, *Cryptojacking*, Desempenho.

Abstract

Technological evolution, associated with new methodologies and procedures for solving human problems, is usually followed by developments in criminal activities. The rise of blockchain and cryptocurrency technologies confers different possibilities for making payments, anonymizing processes and investments, supporting also a new opportunity for malicious agents to generate illicit ways of earning income.

One result of this normalization is cryptojacking, which belongs to the lucrative malware category and means the introduction of malicious code into local programs or online sites, in order to divert processing power from affected devices for unauthorized cryptocurrency mining. For the first time, the incidence of this type of malware has surpassed that of ransomware, making relevant the study of the phenomenon, the understanding of the problem and the analysis of its characteristics.

In this respect, the present work consists in properly instate this malware in the theoretical framework, complemented by a practical part in which experiments were performed, in controlled environment, with different variables and properties, to analyze and measure the effects of cryptojacking on the performance of a computer system.

This study concludes that: there are several types of illicit mining scripts running in websites' code; it is possible to assume the presence of cryptojacking through the affected system performance analysis; there is a direct relationship between CPU percentage utilization and malware activation; the temperature recorded after each test is also indicative of unwanted mining activity.

Keywords: Cryptocurrency, Malware, Cryptojacking, Performance.

Conteúdos

Lista de tabelas

Lista de figuras

Lista de abreviaturas, siglas e acrónimos

ASIC	Application-Specific Integrated Circuit
CAPEC	Common Attack Pattern Enumerations and Classification
CPU	Central Processing Unit
DDoS	Destributed Denial of Service
ENISA	European Network and Information Security Agency
GB	Gigabyte
GPU	Graphics Processing Unit
IA	Inteligência Artificial
IoT	Internet of Things
IST	Instituto Superior Técnico
Kbit	Kilobit
MD	Monitor de Desempenho
MV	Máquina Virtual
p. ex.	Por exemplo
p.	Página
SO	Sistema operativo
SSD	Solid State Drive
Tf_c	Temperatura final, em graus Celcius
TV	Televisão
URL	Uniform Resource Locator
US-CERT	United States Computer Emergency Readiness Team
v_m	Velocidade de transferência média, em Kbit/s
$\%CPU_{máx}$	Percentagem de utilização máxima da CPU
$\%CPU_{mín}$	Percentagem de utilização mínima da CPU
$\%CPU_m$	Percentagem de utilização média da CPU
$\%GPU_{máx}$	Percentagem de utilização máxima da GPU
$\%GPU_{mín}$	Percentagem de utilização mínima da GPU
$\%GPU_m$	Percentagem de utilização média da GPU

Capítulo 1

Introdução

O presente trabalho insere-se na estrutura curricular dos cursos ministrados no Instituto Superior Técnico (IST) e assume-se com o caráter formal de Dissertação de Mestrado, tendo por objetivo a obtenção do grau de Mestre em Segurança de Informação e Direito no Ciberespaço, num curso coordenado pelo IST, em colaboração com a Faculdade de Direito da Universidade de Lisboa e com a Escola Naval.

A este propósito, cumpre-se a realização de um estudo subordinado ao tema "Identificação e Análise de *Cryptojacking*: efeitos no desempenho", constatando-se a sua pertinência pelo significativo aumento de interesse generalizado em criptomoedas, em parte pela segurança e anonimização que este tipo de moeda confere em trocas comerciais ou pagamentos, e por outro lado porque ocorreu uma valorização muito considerável de algumas dessas moedas, que passaram a assumir preferência de investimento, em detrimento de outros ativos no mercado de risco.

A este respeito e à semelhança do que ocorre em praticamente todas as áreas, alguns criminosos do mundo virtual também evoluíram para acompanhar estas recentes tendências, pelo que o surgimento do *cryptojacking*, um tipo de *malware* de deteção difícil e que pode afetar praticamente qualquer sistema ligado à internet, não derivou diretamente do aparecimento de novas técnicas ou do desenvolvimento tecnológico, tratando-se sim de uma evolução ou resultado natural, proveniente das recentes oportunidades de negócio e de mineração de moedas digitais (Wolfson, 2018). Por sua vez, para ser rentável (atendendo ao consumo de energia inerente ao processo), a mineração implica uma elevada capacidade de processamento, que pode ser conseguida particularmente, através de *hardware* eficaz, mas com custos avultados, ou pela alternativa, mais comunitária e sustentável, de se utilizar um equipamento menos apto, integrando um sistema de mineração paralelo e distribuído por diversas máquinas, combinando o seu poder de processamento e dividindo os lucros obtidos pelo conjunto (Rauchberger *et al.*, 2018).

Note-se que, desde finais de 2017, o número de infeções por *cryptojacking*, que atua, sobretudo, através do comprometimento de sites, roubando poder de processamento aos seus visitantes, tem vindo a aumentar vertiginosamente, tornando-se uma das maiores ameaças registadas em 2018, assinalando assim a sua presença em diversos relatórios de agências de segurança de informação, como a Cyber Threat Alliance (2018), bem como de empresas privadas de cibersegurança, como a Symantec (2018), sendo considerada, de momento, uma ameaça tanto ou mais significativa do que a última grande estirpe – o *ransomware* (Lopatin, 2018).

Derivado da sua contemporaneidade, trata-se de uma matéria que se encontra em estado de estudo e exploração, não se dispondo ainda de uma bibliografia extensa e precisa que identifique ou aborde todas as questões essenciais, que sirvam de suporte à investigação e auxiliem o seu enquadramento.

Começa-se por fazer o enquadramento teórico de várias temáticas importantes e adjacentes, sobretudo através da exposição de vários tipos de *malware*, introdução e explicação generalizada do funcionamento da *blockchain* e das criptomoedas. Posteriormente coloca-se a ênfase no objeto principal de estudo, explorando o tipo específico de *malware* designado *cryptojacking*, com a finalidade de identificar e compreender o "estado da arte" no que diz respeito ao surgimento deste novo tipo de ameaça, quais as suas formas de atuação e que efeitos potenciais podem vir a manifestar nas máquinas das vítimas.

Numa primeira abordagem, pretende-se efetuar a pesquisa bibliográfica necessária e adequada ao enquadramento de vários tipos de *software* maliciosos, nos quais se identificará também o *cryptojacking*. Posteriormente, tenciona-se analisar concretamente as formas de atuação de alguns destes *malwares* e, em *ultima racio*, se as condições necessárias o permitirem, testar e comparar as suas potencialidades e efeitos no desempenho de programas, dispositivos ou outros sistemas afetados, com base nos dados recolhidos e publicados por entidades, empresas e organismos que atuem na área da cibersegurança, bem como, por experimentação.

Considera-se que, a partir deste ponto crucial, o presente trabalho será no sentido de dar cumprimento às seguintes finalidades de investigação:

- Enquadrar corretamente o *cryptojacking* no contexto geral dos *malwares*;
- Identificar e analisar as várias estirpes de *cryptojacking* existentes atualmente;
- Caraterizar, comparar e relacionar os *malwares* de *cryptojacking* com maior significância;
- Identificar os fatores e os efeitos associados à utilização de *cryptojacking*.

Para atender ao exposto, é essencial apresentar algumas questões de partida, formular hipóteses de resposta e, por conseguinte, desenvolver extensamente todos os capítulos e subcapítulos de forma integrada, para no final tecer conclusões que permitam verificar as suposições criadas e a sua congruência com a realidade.

Consequentemente, vislumbra-se a seguinte questão de partida, da qual se extraem algumas questões derivadas e respetivas hipóteses:

Quais as principais caraterísticas do *cryptojacking*, a sua relevância atual e os efeitos que provocam no sistema afetado?

Questão Derivada n.º 1: Quais os fatores associados à evolução e disseminação do *cryptojacking*?

Hipótese n.º 1.1: O valor de mercado das criptomoedas.

Hipótese n.º 1.2: O grau de dificuldade de mineração.

Questão Derivada n.º 2: Qual a significância dos vários tipos de *cryptojacking* para o desempenho do dispositivo afetado?

Hipótese n.º 2.1: Alguns *malwares* de *cryptojacking* atuam de diferente modo, consoante as particularidades do sistema/*browser* afetado.

Hipótese n.º 2.2: Quanto menor o efeito no desempenho do dispositivo da vítima, mais difícil será a deteção do ataque.

Questão Derivada n.º 3: É possível detetar um ataque de *cryptojacking*, pela análise de desempenho do sistema afetado?

Hipótese n.º 3.1: Para a mineração ser eficaz e lucrativa, a forma como o desempenho da CPU ou da GPU é afetado por essa atividade, apresenta padrões reconhecíveis.

Hipótese n.º 3.2: Existem outros fatores que podem provocar os mesmos sintomas nos sistemas.

Questão Derivada n.º 4: Para além da análise ao desempenho da CPU ou da GPU, existem outras variáveis pertinentes para a deteção do *cryptojacking*?

Hipótese n.º 4.1: É relevante atender à temperatura atingida pelo sistema.

Hipótese n.º 4.2: É relevante considerar a velocidade de transferência de dados entre o sistema e a internet.

No sentido de conseguir concretizar o estudo em consideração na sua plenitude, será seguida uma abordagem repartida em duas partes: uma teórica, de reunião e revisão bibliográfica; e outra prática, de experimentação, registo e comparação de resultados.

A metodologia seguida para a **parte teórica** inicia-se pela análise documental, baseada em artigos de revistas científicas, livros, monografias, teses de doutoramento, dissertações de mestrado, notícias de fonte segura e reconhecida, bem como de outros documentos relevantes. Nesta parte, procura-se responder às hipóteses do ponto de vista doutrinário, sendo a investigação executada por fases, conforme seguidamente se irá discriminar:

1.ª Fase: Com base na literatura de referência, procura-se caraterizar e diferenciar os vários tipos de *malware*, explicando os seus conceitos e enquadrando o *cryptojacking*, em específico, de forma a identificar as diferentes alusões e, assim, conduzir a investigação para os aspetos essenciais à consecução dos objetivos do presente trabalho;

2.ª Fase: A partir da literatura de referência, analisam-se os vários conceitos que se relacionam com o *cryptojacking*, dando também aso à explicação da *blockchain* e da existência e história das criptomoedas;

3.ª Fase: A partir do resultado da análise documental, serão identificados os principais tipos de *cryptojacking* atuais e efetua-se a sua explicação;

4.ª Fase: Com base em todas as referências teóricas selecionadas, tenta-se responder à Questão de Partida e às derivadas;

A **parte prática** contemplará as seguintes fases:

1.ª Fase: Seleção dos tipos de *cryptojacking* mais significativos atualmente, de acordo com a pesquisa teórica;

2.ª Fase: Testar a influência desses *malwares* no desempenho de algumas componentes de um computador portátil, a correr diferentes sistemas operativos (SO);

3.ª Fase: Comparar resultados e complementar as respostas prévias à Questão de Partida e derivadas, comprovando ou reprovando as hipóteses formuladas.

O presente trabalho encontra-se estruturado da seguinte forma:

- Capítulo 1 – Introdução – apresenta o trabalho, a questão de partida, as questões derivadas e respetivas hipóteses de resolução, mencionando ainda a pertinência e os objetivos do estudo;
- Capítulo 2 – Contextualização e trabalho relacionado – efetua o enquadramento geral ao trabalho e aborda especificamente a bibliografia e as descobertas relacionadas com as temáticas em apreço, concretamente acerca de *malware*, *blockchain*, criptomoedas e *cryptojacking*;
- Capítulo 3 – Metodologia – menciona os pormenores propostos para a realização da parte prática, bem como o modelo metodológico seguido;
- Capítulo 4 – Influência do *cryptojacking* no desempenho – contém os detalhes e resultados das experiências realizadas;
- Capítulo 5 – Conclusão – apresenta as considerações finais do trabalho e as propostas para estudos futuros;
- Referências bibliográficas – integra o registo de todas as fontes bibliográficas, citadas ao longo dos conteúdos dos capítulos mencionados;
- Apêndices – agregam toda a informação pertinente, relacionada com o trabalho e proveniente do autor, mas que não seria exequível incluir nos capítulos principais.

Capítulo 2

Contextualização e trabalho relacionado

O crescente número de hipóteses tecnológicas para facilitação e resolução de tarefas pessoais ou laborais, constitui-se igualmente como a janela de oportunidade para agentes mal-intencionados poderem pensar e desenvolver novas formas de atuação que se reflitam em proveito próprio ou das suas organizações.

Com o dado adquirido de que os ciberataques vieram para ficar, Barnum e Sethi (2007) afirmaram, à data, que construir *software* com o nível de segurança adequado, era uma missão cada vez mais desafiante, uma vez que a dimensão e complexidade dos programas exigidos era cada vez maior e os atacantes continuavam a conseguir encontrar vulnerabilidades. Numa perspetiva mais atual, Tabone (2017) corrobora essa visão, mencionando que se têm introduzido outras formas de ataque ao ciberespaço, diferentes das convencionais e que o espectro de ameaças e motivações para esses ataques evolui continuadamente, passando-se, por exemplo, de ataques para criar reputação ou exclusivamente com fins recreacionais, para ataques com propósitos financeiros, ideológicos (*hacktivism*), políticos ou terroristas. Outros autores referem inclusivamente que os piratas informáticos estão a progredir mais rápido do que a tecnologia em si, fundamentando-se no facto do número de ataques e novas ameaças, em computo geral, não estagnar ou reduzir (Siciliano, 2018), ou numa vertente mais futurista, que as capacidades desses agentes se vão potenciar, expandir e readaptar para acompanhar a tendência de incorporação da Inteligência Artificial (IA) na vida humana – como será o caso dos dispositivos integrados em IoT (traduzido, Internet das Coisas) (Ismail, 2018).

Inúmeros tipos de ataques, relacionados com as tecnologias de informação podem ocorrer e têm sido descritos, mas alguns dos mais significativos, que contemplam alvos individuais ou organizacionais, são designadamente: ataques distribuídos de negação de serviços (DDoS), que tornam determinado recurso indisponível para os utilizadores legítimos; ataques *phishing* ou *spear-phishing*, nos quais o criminoso tenta adquirir informações importantes do alvo, para posteriormente as utilizar; engenharia social, que se afigura como um método prático e eficaz de obtenção de informação crítica, tal como dados de identificação ou bancários, através de interação direta com o alvo ou um terceiro; quebras de dados (*data breaches*), que podem expor grande quantidade de informação privada dos seus alvos; e *malware*, que pode materializar-se pelas mais variadas formas de *software* e produzir efeitos diversos, consoante o seu propósito e a intenção do criminoso (Yadav e Gour, 2014).

Em resposta a quais os maiores desafios de cibersegurança enfrentados atualmente, a Cisco (2018a) responde no seu Cybersecurity Special Report, que têm sido os ataques dirigidos a colaboradores específicos de empresas para aquisição de informação (*spear-*

physhing), o *ransomware* e as ameaças avançadas persistentes, representadas por *malware* avançado e que ainda é desconhecido.

Um recurso online aberto e digno de menção para análise extensiva destas ameaças é o Common Attack Pattern Enumerations and Classification (CAPEC), que auxilia toda a comunidade especializada e de internautas comuns a identificar e entender os ataques no ciberespaço, apresentando uma lista bastante completa dos mecanismos de ataque conhecidos, aos quais atribui um código específico e subdivide por categorias, consoante o padrão seguido, a técnica utilizada ou a metodologia adotada (CAPEC, 2018).

Seguidamente, pretende-se efetuar um enquadramento geral ao *software* malicioso, e depois explicar o funcionamento da *blockchain* e das criptomoedas, terminando-se com a alusão à problemática concreta do *cryptojacking*.

2.1. *Software* malicioso

O *software* malicioso, comummente designado por *malware*, é descrito como sendo *software* que cumpre deliberadamente as intenções negativas/prejudiciais de um atacante (Egele *et al.*, 2012) e pode materializar-se através de qualquer programa computacional que funcione contrariamente à vontade ou interesse do utilizador ou proprietário de um sistema. Atualmente, as formas e os tipos possíveis de registo de *malware* são inúmeros, gerando a discussão entre especialistas para comprovar a sua existência e proceder à respetiva identificação e catalogação (Eilam, E. 2011).

No que concerne à categorização de *malware*, a visão de Rutkowska (2006), à época, referia que esta se baseava no comportamento apresentado e nos resultados produzidos. Mais recentemente, numa linha de pensamento mais abrangente, Suleiman e Husain (2015) classificam *malware* de acordo com os seguintes critérios de taxonomia: meio de difusão, que se subdivide em transmissão baseada no sistema (que exige ação ou atividade humana e ocorre, p. ex., durante os contactos de um sistema com suportes de multimédia móveis) e transmissão baseada na rede, usualmente auto-replicada; natureza do dano, podendo os efeitos malignos verificar-se logo a partir da infeção, a curto prazo ou a longo termo; e o *malware intelligence*, que pode ser estático, no caso do programa infecioso manter a sua forma primária, ou dinâmico, se tiver dependências de outros programas ou funções de reprogramação.

Outras classificações taxonómicas podem ser consideradas, nomeadamente as relacionadas com ciberguerra, que incluem critérios diferentes, mas igualmente válidos. Nesta área, são apontados: a discricionariedade (*stealth*), indicando que é determinante para a sua propagação, subdividindo-a em cinco níveis, desde o mais básico e que se dissemina tradicionalmente como um vírus comum, espalhando-se agressiva e ativamente, ao mais evoluído e aprimorado, que opera subtilmente em alvos selecionados, dissimula-se no sistema e possui capacidade para evitar a deteção; a destrutividade, também distribuída por níveis,

desde o *malware* praticamente inofensivo, passando pelo capaz de prejudicar o desempenho ou eliminar ficheiros, até ao que cifra *software* ou provoca danos persistentes em *hardware*; e a capacidade de monitorização e aquisição, variando do que não extrai quaisquer dados, até ao que consegue recolher quantidades significativas de informação relevante, como credenciais de acesso, documentos específicos, ou extensos conjuntos de dados ao nível de exames forenses (Hurley e Chen, 2018).

No que diz respeito à arquitetura, por norma, o *malware* que afeta dispositivos computacionais enquadra-se através de quatro pontos principais: o mecanismo de infeção, que pode variar entre uma seleção aleatória ou selecionada através de suportes multimédia físicos ou por intermédio da rede/internet; o mecanismo de disseminação, que enquadra sobretudo a auto-propagação, aquando do contacto inicial com o sistema vulnerável, a propagação embutida através de canais normais de comunicação (como o e-mail), ou ainda a propagação por canal secundário, infetando primariamente a vítima e efetuando a transferência e ativação do *malware* já a partir da mesma; o mecanismo de ativação, que pode ser automática (pela exploração de vulnerabilidades do sistema), manual por ação humana (p. ex., pelo clique numa hiperligação), baseada em determinada atividade humana insuspeita (p. ex., pela inserção de um suporte de multimédia ou aquando de uma autenticação), ou por processos agendados; e, por fim, a natureza do ataque, que pode materializar-se em roubo de dados, controlo completo ou de funções do sistema atingido, modificação ou cifração de ficheiros, ou até produção de dados físicos e inutilização do sistema ou dos seus componentes (Suleiman e Husain, 2015).

Apesar da dificuldade na sua documentação formal, têm sido referidos frequentemente, ao longo dos anos, vários tipos de *malware*, consoante as caraterísticas apresentadas, o método utilizado e o propósito adjacente. Atualmente, em alusão às fontes bibliográficas da Tabela n.º 1, pode afirmar-se que tipos referidos com maior frequência são:

- Vírus – que se traduzem por programas que se auto-replicam e infetam outros programas ou ficheiros;
- *Spyware* – que são colocados secretamente numa máquina alvo sem a permissão do utilizador e, como o nome indica, têm o objetivo de vigiar a atividade desencadeada, reunindo informações relevantes que, em tempo real ou à posteriori, são devolvidas ao agente mal-intencionado;
- *Adware* e *spambots* – que têm vindo a ganhar popularidade desde os primórdios da internet e que, embora não apresentando consequências graves para as vítimas, as infesta com *pop-ups* publicitários indesejados e sem a possibilidade de os controlar ou remover;
- *Rootkits* – que podem ser bastante difíceis de detetar e permitem a um agente mal-intencionado aceder ou controlar remotamente uma rede ou dispositivo terceiro, sem a permissão do seu utilizador legítimo;
- *Backdoors* – que, através do compromisso de um sistema, permitem obter permissões de acesso ilegítimas e sem o conhecimento do utilizador principal;

- *Trojans* – que de forma similar à lenda grega do ataque a Tróia, são programas maliciosos que aparentam ser fidedignos, para que o seu utilizador os aceite e instale de livre vontade;
- *Worms* – que se replicam, à semelhança dos vírus convencionais, diferindo porque se alastram a outros dispositivos através da rede, ao invés de permanecerem ligados a um programa ou código executável específico no sistema em que se instalaram;
- *Ransomware* – que, tal como se interpreta pelo próprio nome, bloqueia determinado sistema ou conteúdo (ficheiros ou programas, regularmente), exigindo o pagamento de uma quantia monetária (ou por transferência ou em criptomoedas) para reaver o acesso;
- *Cryptojacking* – que empregam o poder de processamento de determinado sistema, por norma em larga escala e sem consentimento dos utilizadores, para aquisição de moedas digitais;
- *Keyloggers* – que funcionam de modo a registar, guardar e, eventualmente, enviar para um agente mal-intencionado, todos os batimentos feitos por um utilizador num teclado, permitindo o roubo de credenciais e outros dados sensíveis sem que a vítima se aperceba;
- *Bot* ou *Remote Access Trojan* (RAT) – que atuam através da aquisição de controlo de uma (ou diversas) máquina(s) de utilizador(es) comum(s), utilizando-se esse acesso posteriormente para organização e lançamento de outro tipo de ataques, como por exemplo, transmissão de outros *malwares*, ataques DDoS, *botnets*, ou disseminar e-mails de *spam* em larga escala.

Há duas técnicas reconhecidas para deteção de *malware*: a baseada em padrões (*signature-based*), representada pela grande maioria dos programas de antivírus e apenas com capacidade de identificação de agentes maliciosos conhecidos ou que integrem um conjunto de regras previamente definido; e a baseada no comportamento (*behavior-based*), assumindo-se que o *malware* pode ser descoberto através da observação dos efeitos nefastos, durante o período em que está a ser executado (Galal *et al.*, 2015).

Ainda assim, não existindo métodos de deteção infalíveis, independentemente do nível de conhecimento do utilizador ou da dificuldade na deteção destes agentes, há alguns sinais e sintomas que devem despertar o alerta e que podem significar a infeção por *malware*, designadamente: SO ou programas que bloqueiem o sistema frequentemente; programas que iniciam ou terminam a sua execução sem interferência do utilizador; alterações drásticas e inesperadas do espaço disponível em disco; cortes no acesso a programas ou ficheiros; maus funcionamentos persistentes de exploradores de internet; redireccionamento de determinadas páginas online para outras; aparecimento de mensagens de alerta ou de publicidade pouco usuais; abrandamento da velocidade geral do computador ou da conexão à internet, bem como de programas ou sites específicos (Kaspersky, 2013).

Em termos estatísticos, a Kaspersky, conhecida empresa russa de cibersegurança, aponta no seu relatório intitulado Kaspersky Security Bulletin 2018, com informações provenientes da recolha e análise de dados de clientes dos seus produtos, que, ao longo do ano transato, cerca de 30% dos computadores que protege, foram alvo de, pelo menos, um ataque

enquadrável na classe de *malware*. É ainda destacado nesse documento que: mais de 800 mil dispositivos foram protegidos, pelos seus serviços, contra *malware* que tentava desviar dinheiro através de serviços bancários online; mais de 750 mil computadores individuais foram alvo de ataques relacionados com cifração de dados; e mais de 5,5 milhões de computadores individuais foram alvo de mineração indesejada (AMR, 2018).

Em par com a disseminação das mais variadas tecnologias e novos meios, também estes *softwares* prejudiciais se têm espalhado de inúmeras formas e manifestam tendência para continuar a aumentar os seus registos.

De seguida, expõem-se na Tabela n.º 1 os vários tipos de código malicioso que representam maior relevância, mediante a sua identificação em artigos atuais e autores de referência, acompanhados de uma descrição sumária.

Tabela n.º 1 – Identificação e descrição dos tipos de *malware* mais significativos na atualidade.

Tipo	Descrição	Fonte
Worm	Com uma forma de atuação similar às dos vírus comuns, são códigos computacionais maliciosos que se replicam, propagam autónoma e automaticamente pelas redes, e apresentam um comportamento repetitivo e previsível, que facilita a sua deteção.	Grimes (2018); Subrahmanian *et al.* (2015); Li *et al.* (2008).
Trojan	Também chamados de *trojan horses*, consideram-se dos substitutos mais utilizados e eficazes aos *worms*, tratando-se de ficheiros ou programas que aparentam ser legítimos, mas que contêm código malicioso escondido. Nestes se inclui, p. ex., o *repackage* (modificação de Aplicações fidedignas).	CAPEC (2018a); Grimes (2018); Subrahmanian *et al.* (2015); Suarez-Tangil *et al.* (2014).
Backdoor	São um dos tipos de *malware* mais comum e materializam-se de várias formas para permitirem obter acesso remoto a um programa ou máquina e funcionalidades como a visualização de ecrã, gestão de diretórios, a procura de ficheiros ou edição de chaves de registo.	CAPEC (2018b e 2018c); Thomas e Francillon (2018); Sikorski e Honig (2012).
Ransomware	Código malicioso, por norma de execução local, que cifram os dados de um sistema e os mantêm inacessíveis, até ser pago um resgate.	CAPEC (2018d); Cisco (2018 e 2018a); Grimes (2018); Subrahmanian *et al.* (2015).
Cryptojacking	Também designado por *coin mining malware* ou *crypto-malware*, é uma das formas mais recentes de utilização de recursos de processamento de máquinas remotas. O seu propósito é adquirir criptomoedas, podendo ser baseado em programas no próprio sistema ou correr através de códigos online.	US-CERT (2018); Cisco (2018a); Kleinman (2018); Lopatin (2018); ENISA (2017).

2.2. *Blockchain* e criptomoedas

As criptomoedas surgem num contexto complexo, com definição conturbada, em par com a própria *blockchain* que sustenta a sua existência. Com o intuito de compreender melhor estes conceitos e a razão que leva alguns autores a afirmar que o futuro passa precisamente pela transposição da economia "real" para a digital, e outros a referir que tal ideia jamais seria concebível, começa-se por explanar estas noções.

A *blockchain*, conhecida pela primeira vez em 2009, num artigo publicado por alguém desconhecido, sob o pseudónimo de Satoshi Nakamoto (Marr, 2018), funciona como uma base de dados partilhada por uma rede mundial de computadores (que se designam por "nós") e que, quando cria um novo registo, torna muito difícil alterá-lo, porque seria necessário fazê-lo em inúmeras máquinas e numa coordenação praticamente impossível. Para assegurar que as cópias da base de dados se mantêm iguais, são feitas confirmações à rede, nas quais se contemplam: os registos, que detêm informação proveniente de novos blocos descobertos (minerados) e os dados derivados de todas as transações feitas, guardando a assinatura digital das partes envolvidas e verificando os detalhes através da rede para garantir que a troca é válida; os blocos, que constituem o conjunto de registos aceites pela rede, contendo um código único (designado *hash*), que permite a sua integração na corrente (*chain*) e incorporam também o código do bloco anterior, ao qual ficam acoplados; e, por fim, a chamada corrente ou cadeia de blocos – a *blockchain* – sendo a parte que engloba e interliga todos os registos e blocos, por uma ordem específica e praticamente inalterável, fazendo com que não seja necessária a autenticação de entidades terceiras e certificadas para garantir a sua inviolabilidade (Murray, 2018).

O fundamento desta rede *peer-to-peer* é que, quem corra o seu código, minerando uma criptomoeda, utilize uma parte significativa do poder de processamento de uma máquina ou conjunto de máquinas, para receber dados das transações que estão a ser efetuadas e os reúna para tentar criar um novo bloco, ao mesmo tempo que mantém uma cópia crucial de todas as outras transações efetuadas, que são registadas com a mesma ordem em toda a rede.

A grande dificuldade deste processo é que, para que o novo bloco seja validado, é necessário providenciar uma prova criptográfica com o mesmo, a qual é obtida através de inúmeras tentativas de resolução, que tornam uma amostra de dados de comprimento arbitrário, num conjunto de carateres alfanuméricos com comprimento fixo (*hash*). Por sua vez, tornando o processo ainda mais desafiante, o algoritmo da *blockchain* exige que a *hash* comece com um determinado número de zeros, que não é possível prever à priori e obriga à execução repetitiva, por tentativa-erro, da operação de transformação destes dados.

A conclusão deste processo com sucesso, a qual aufere uma remuneração ao minerador que a descobrir, dá-se somente quando é encontrada uma *hash* satisfatória, a qual é de seguida anunciada à rede e incorporada no final da versão da *blockchain* que cada utilizador possui. Por este motivo, trata-se de uma rede bem alicerçada e, apesar de, teoricamente, ser corruptível, na prática seria um processo muito complexo, sobretudo numa *blockchain* com

muitos nós, uma vez que seria necessário penetrar e alterar todas as cópias existentes, num dado momento, para conseguir realizar operações novas fraudulentas ou tentar realizar várias vezes a mesma transação (Peck, 2017).

Afigura-se ainda relevante mencionar que a rede está concebida de forma a ajustar a complexidade de mineração dos blocos seguintes, seguindo-se uma lógica de aumento de dificuldade e de exigência do poder de computação, à semelhança do que, em teoria, ocorre com recursos naturais valiosos: à medida que vão sendo descobertos poços de petróleo, reduz-se a probabilidade de encontrar outros; o mesmo ocorre com minerais, como ouro ou prata. Esta componente do processo é fraturante, pois implica que, mesmo os utilizadores comuns e que tencionam apenas "extrair" algum rendimento extra através dos meios que têm, se vejam obrigados a aderir a grupos (*pools*) online, para conseguir alguma compensação efetiva, que será calculada de acordo com as regras do proprietário e poderá depender do seu contributo individual (Xie, 2018).

Apesar da *blockchain* ter sido inicialmente concebida com o olhar focado em criar moedas digitais seguras para todos, e alguns autores (talvez, a maioria) defendam a perspetiva de uma *blockchain* plenamente funcional e com diversas aplicações benévolas no futuro, é referido também por outros, que há potencial para aplicações negativas dessa tecnologia. A esse propósito, Rossow (2018) refere que a tecnologia de *blockchain*, combinada com outras tecnologias recentes e ainda subdesenvolvidas, como a IA, podem contribuir para a inovação na aquisição de informação em larga escala, na renovação do setor energético (cidades inteligentes), ou ainda na criação de robots ou *chatbots*.

Marr (2018), numa visão dualista, acrescenta tratar-se de "um grande sistema eletrónico, sobre o qual se podem construir aplicações", destacando que embora a *blockchain* esteja intimamente ligada à criação do Bitcoin (BTC), permitindo a sua existência, é independente dessa moeda digital e pode ser empregue de forma revolucionária na indústria financeira e em instituições educativas.

Por outro lado, Marr (2018a) não deixa também de apontar algumas consequências negativas desta tecnologia, alertando para alguns problemas que podem advir da sua utilização, nomeadamente: os de cariz ambiental, uma vez que cifração avançada e descentralizada exige grande poder de computação, que por sua vez requere quantidades de energia avultadas; o facto de poder tornar-se um processo lento e "pesado", igualmente pelos motivos referidos no ponto anterior, o que provoca um atraso maior do que o esperado, como p. ex., para uma simples transação monetária; os efeitos derivados da falta de regulamentação ou legislação, que tornam arriscado o envolvimento e compromisso para com essa temática; a sua elevada complexidade, fazendo com que seja difícil os utilizadores comuns compreenderem a sua verdadeira utilidade e capacidade; e o desejo, por parte de entidades e organismos poderosos, como as instituições bancárias, que têm um interesse muito particular em que essa tecnologia não seja desenvolvida, visto poder vir a substituir o seu papel de intermediários e certificadores em inúmeros processos e operações financeiras.

No que diz respeito aos efeitos colaterais do desenvolvimento da economia digital, e apesar das opiniões diferirem, existindo base de sustentação para ambas as partes, a verdade é

que as criptomoedas já afetaram a economia e os mercados financeiros de alguns países. Observe-se a intenção manifestada por alguns Bancos de proibir o depósito de fundos provenientes do câmbio de criptomoedas ou impedir a sua compra com determinados cartões bancários (Aslam, 2018), ou o caso de uma *startup* suíça reúne o equivalente a mais de 100 milhões de dólares americanos para abrir um "criptobanco" (Neghaiwi, 2018), ou ainda o esclarecimento de Carlos Costa (*cit in* Lusa, 2018), Governador do Banco de Portugal, ao afirmar que "criptomoedas não são moedas, são ativos cujo valor pode oscilar em função do subjacente e em função da crença que os participantes do mercado têm no seu valor futuro".

Por outro lado, há o relato de Sen (2017) à agência financeira Bloomberg, em que menciona que a gigante oscilação no valor de criptomoedas, já conhecidas do público geral, se constitui também como uma referência futura para os consumidores e as empresas investirem em novas criptomoedas, que pela lógica da oferta/procura começarão com valores irrisórios e terão um enorme potencial de crescimento.

De forma similar, existem ainda outras perspetivas mais otimistas e visionárias, como a de Parreira (2018), referindo que a influência das moedas digitais e o desenvolvimento da tecnologia de *blockchain* podem ter um impacto positivo nas economias, conseguindo traduzir-se no reforço do mercado laboral esporádico, como o caso do setor de consultoria, e ainda na criação de novos empregos efetivos nas áreas de informática, segurança de informação e gestão e autenticação de processos ou bases de dados.

Desde 2009, para além do Bitcoin, outras moedas digitais foram surgindo e marcando a sua quota parte no mercado de transações online e de investimento, sendo de referir algumas, criadas entre 2011 e 2017: Litecoin (LTC), Ripple (XRP), Monero (XMR), Stellar (XLM), Ethereum (ETH) e Bitcoin Cash (BCH). Os factos são que, algumas das moedas referidas anteriormente, como o caso concreto do Bitcoin (Figura n.º 1), do Ethereum (Figura n.º 2) e do Monero (Figura n.º 3), embora com importâncias absolutas bastante díspares, apresentaram uma valorização recorde entre os meses finais de 2017 e o início de 2018, finda a qual voltaram a ver os seus valores reduzir novamente, confirmando-se a inconstante flutuação.

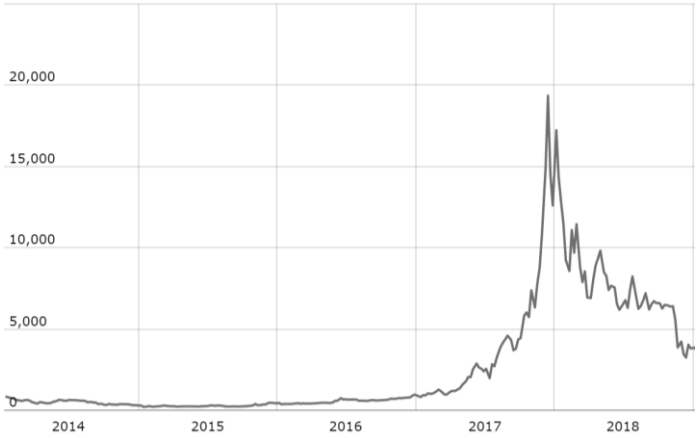

Figura n.º 1 – Variação do valor de Bitcoin desde a sua criação até ao final de 2018, em dólares americanos (WorldCoinIndex, 2018).

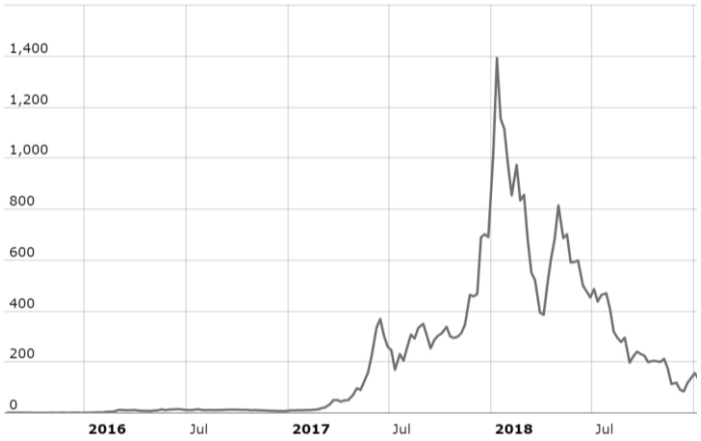

Figura n.º 2 – Variação do valor de Ethereum desde a sua criação até ao final de 2018, em dólares americanos (WorldCoinIndex, 2018a).

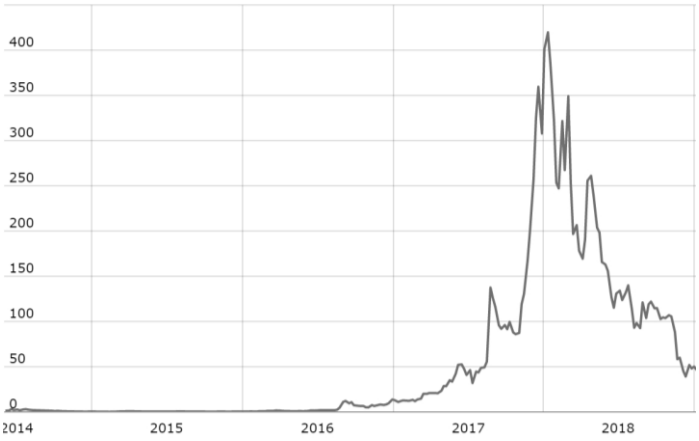

Figura n.º 3 – Variação do valor do Monero desde a sua criação até ao final de 2018, em dólares americanos (WorldCoinIndex, 2018b).

Mesmo assim, este súbito crescimento no valor e na consequente procura por moedas digitais, descrito no Relatório de Ameaças à Segurança da Internet de 2018, pela Symantec (2018, p. 19), como a "corrida ao ouro" moderna, levou à ocorrência de diversas situações pouco comuns, tais como:

- O aumento considerável desse mercado para fins de investimento, inclusive em detrimento dos investimentos convencionais, e sobretudo junto dos estratos mais jovens ou de quem está ligado ao mundo tecnológico e considera esta aposta como tendo grande potencial recompensador (Arnold, 2018);
- A aceitação de pagamentos (ou permutas) em Bitcoin, para aquisição de vários produtos, bens ou serviços, incluindo casas no mercado imobiliário português (Pinheiro *et al.*, 2018);
- A difusão e instalação, em locais estratégicos de algumas cidades, de máquinas de câmbio e levantamento de moedas digitais (SAPO TEK, 2018);

- A rotura de stock, a nível mundial e por vários meses, de determinadas placas gráficas de marca Nvidia e AMD, assim como de outros equipamentos mais específicos (ASICs ou *mining-rigs*) e com atributos lucrativos para mineração (Evangelho, 2018).

Salienta-se também, que no início de 2018 e pela primeira vez na história mundial, um país – a Venezuela – fundou e declarou a sua moeda digital, o Petro, como moeda oficial do país e assente nos valores da sua economia, com base nas reservas de petróleo detidas. Num aparente rasgo de confiança, apesar de se tratar da moeda digital criada por uma economia enfraquecida e em forte recessão desde 2017 (Laya, 2019), cerca de 130 outros países demonstraram interesse em investir no Petro, representando um total de mais de 200 mil ofertas e um montante inicial de cerca de cinco biliões de dólares americanos (Aitken, 2018). Para além de benefícios políticos e económicos subjacentes, este interesse aparenta demonstrar que, mesmo com as incertezas inerentes a estes mercados, pessoas e Estados não querem ficar para trás e perder a oportunidade de integrar a revolução das moedas digitais.

2.3. *Cryptojacking*

Tal como referido e acompanhando as propensões do mundo digital, nomeadamente as que envolvem rendimentos ou potenciam lucros, também os criminosos tentam tirar proveito de todas as oportunidades ou falhas que encontrem e que lhes permitam obter vantagem económica para os fins mais diversos. A este propósito, a Cisco (2018) indica que o cibercrime tem vindo a aumentar anualmente, com os criminosos a beneficiar de vulnerabilidades (algumas já conhecidas) nos sistemas que permitem que, no caso específico dos ataques *ransom*, 53% resulte em danos económicos superiores a 500 mil dólares.

Voltando a sua atenção para outra nova modalidade, peritos da Cisco (2018a, p. 5) afirmam num relatório ainda mais recente que há outras ameaças que não podem ser ignoradas, focando-se particularmente no *illicit cryptocurrency mining*, o qual é descrito como "uma atividade altamente lucrativa, em que o retorno (fruto da mineração) não pode ser rastreado e que ainda permite que os criminosos se possam abstrair mais da sua responsabilidade criminal", dado que as suas ações não colocam em risco bens ou valores essenciais e são, por sua vez, bastante mais brandos nos seus efeitos e, por esse motivo, mais difíceis de detetar.

A Symantec aponta o retorno e o crescimento acelerado da mineração, comparando as poucas criptomoedas existentes em 2013, que capitalizavam um valor total de mercado de cerca de 1 bilião e meio de dólares, com uns contrastantes 166 biliões, repartidos por mais de 1000 criptomoedas diferentes, registados em finais de 2017, e que potenciaram a mineração e o virar de atenções para os potenciais lucros do *cryptojacking* (Lau, 2017).

Como comparação, o primeiro *ransomware* conhecido mundialmente – denominado WannaCry – começou a sua expansão em 12 de maio de 2017 através de um hospital britânico, alastrando-se posteriormente a mais de 200 mil outras instituições, entre as quais outros hospitais, bancos, organizações governamentais e empresas privadas, colocando vidas humanas em perigo, causando prejuízos económicos avultados para as vítimas (Jones, 2017), tendo um impacto considerado com escala "sem precedentes" pela Europol (BBC, 2017), mas com ganhos muito reduzidos para os atacantes, de cerca de 50 mil dólares em Bitcoins nos primeiros 3 dias (Karphal, 2017).

Em complemento, o relatório Kaspersky Security Bulletin 2018 reitera que, pela primeira vez nos registos, nesse ano, os *malicious cryptocurrency miners* sobrepuseram-se à maior ameaça dos últimos anos ao ciberespaço – precisamente os *ransomwares*. O mesmo documento indica que, nos três primeiros trimestres de 2018, mais de cinco milhões de pessoas foram alvo de ataques envolvendo mineração involuntária, sobretudo devido à instalação e utilização de programas não licenciados, o que acabou por representar um aumento vertiginoso desse tipo de ataques face ao mesmo período do ano anterior (Lopatin, 2018).

Acompanhando a tendência, também a McAfee (2018) incide nesta ameaça, apontando no seu relatório, publicado em setembro, que a quantidade de *crypto mining malware* aumentou vertiginosamente desde o início do ano de 2018, registando um aumento destes ataques em mais de seis vezes face ao último trimestre do ano transato.

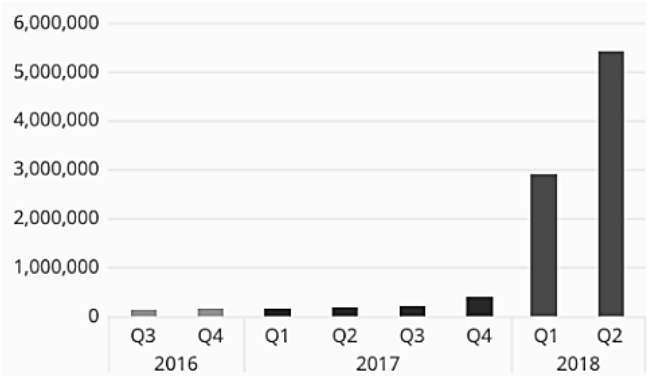

Figura n.º 4 – Quantidade total de *malware* relacionado com mineração de criptomoedas, entre o terceiro trimestre de 2016 e o segundo trimestre de 2018 (McAfee, 2018).

Como se pode verificar, os valores do gráfico presente na Figura n.º 4 vão ao encontro do apresentado nas Figuras n.º 1, 2 e 3, uma vez que fazem coincidir a grande valorização de criptomoedas entre finais de 2017 e primeiros meses de 2018, com o aparecimento e aumento de *cryptojacking*, justificando-se facilmente esse desenvolvimento com a rentabilidade de ter uma rede alargada de máquinas a trabalhar continuamente, aparentemente de forma normal, mas com processos a correr no *background*, ou através do simples acesso de um dispositivo a um site na Internet que começa a correr código automático por JavaScript aquando da sua abertura, com a finalidade de minerar moedas digitais para a carteira digital de uma terceira pessoa, que reunirá todos os lucros que daí provenham.

No que diz respeito à sua forma de atuação, existem duas possibilidades – *cryptojacking* baseado na máquina (*machine-based*, que atua através de *software* instalado localmente no dispositivo, incluindo o sistema operativo) e *cryptojacking* baseado na *web* (*web-based* ou *browser-based*, que toma parte através do simples acesso a um site comprometido) – embora ambos necessitem de ligação à internet e este último seja amplamente mais difundido e explorado, sobretudo pelo seu potencial mais abrangente. Apesar disso, o *software* de mineração pode ser distribuído e inserido com recurso a outros meios, salientando-se: inserção do código malicioso em *software*, aparentemente certificado, e disponível para transferência na internet; disseminar, em larga escala, o *malware* através de listas de e-mails conhecidos; pelas redes sociais, com recurso a técnicas de engenharia social e outras assentes nas fraquezas do fator humano (Bissaliyev *et al.*, 2018).

Segundo Rauchberger *et al.* (2018), a mineração de criptomoedas com base na internet existe, pelo menos, desde 2011, remetendo para um serviço inovador lançado à data, alojado no site `www.BitcoinPlus.com`, que surgiu pelo valor reduzido do Bitcoin na altura, aliado à facilidade de mineração. Mais tarde, em setembro de 2017, deu origem ao CoinHive, serviço similar, que também consiste na utilização de código em JavaScript para mineração em grupo (neste caso, de Monero), através de *mining pools*, permitindo ainda aos utilizadores embutir esse código nos seus sites para que os visitantes minerassem para si.

A Equipa de Prontidão de Emergência de Computadores dos Estados Unidos da América (US-CERT, 2018), por ocasião do crescente ganho de popularidade das criptomoedas, emitiu uma nota de segurança respetiva a este assunto, na qual dá resposta a várias questões primordiais, assim como explica em que consiste o *cryptojacking*, deixando algumas dicas de prevenção ou defesa dessa ameaça. A Equipa começa por referir que o fenómeno ocorre quando agentes mal-intencionados instalam ilicitamente *malware* de mineração nos dispositivos e sistemas das vítimas (através da exploração de falhas em aplicações móveis transformadas, *botnets* e plataformas de redes sociais), ou ainda quando as vítimas acedem a um site ou se conectam a uma rede sem fios comprometida, conseguindo posteriormente alocar a capacidade de processamento dessas máquinas para ganhar criptomoedas. A forma como o *malware* de *cryptojacking* se comporta pode diferir entre ser não-persistente, no caso da mineração não desejada ocorrer somente enquanto o utilizador tem o seu *browser* aberto especificamente na página que está afetada, ou ser persistente, se a atividade de mineração se mantém, mesmo depois da vítima deixar de visitar a página que lhe deu origem ou parar a sua atividade.

São também abordados os dispositivos que são suscetíveis de sofrer algum tipo de ataque relacionado com *malware* de mineração, referindo-se que os mais afetados são sistemas computacionais (computadores e servidores), dispositivos de rede (modems e routers), dispositivos móveis (smartphones, tablets, *smartwatches* e outros sujeitos às mesmas vulnerabilidades que os computadores) e os dispositivos interligados no âmbito de IoT (*smart* TVs, impressoras, câmaras fotográficas ou de vídeo, etc.), concluindo-se que praticamente qualquer máquina com um processador e que esteja conectada à internet é um alvo potencial (US-CERT, 2018).

Apesar da dificuldade de deteção do *cryptojacking* sem ferramentas de análise avançadas, ou sem alguma atenção aliada a conhecimentos informáticos, costumam apresentar-se como consequências dessa atividade:

- A degradação do desempenho do sistema e o aumento do tráfego de rede, uma vez que, os recursos de processamento passam a ser monopolizados pela mineração e a largura de banda também poderá alterar-se ligeiramente;
- O aumento efetivo da temperatura do sistema derivado do esforço intensivo da máquina, que leva a um incremento no consumo de energia (que acarreta um acréscimo dos custos de eletricidade), que pode provocar *crashes* de sistema e que, ainda incorre, no risco potencial de provocar danos físicos em algumas componentes de *hardware*;
- Eventuais perturbações no normal decorrer das operações computacionais;
- Possível prejuízo financeiro, decorrente de falhas de programas ou componentes, que podem levar a que o sistema fique em baixo, intermitentemente funcional ou necessite de ser restaurado.

Também a Agência da União Europeia para a Segurança da Rede e da Informação (ENISA, 2017), menciona que foram detetados vários casos de abuso de criptomineração, com especial enfoque no primeiro código malicioso de mineração conhecido, designado CoinHive, descrito mais adiante no trabalho, e que pode atuar por injeção em JavaScript num site para mineração da criptomoeda Monero.

Segundo a Agência da União Europeia para a Segurança da Rede e da Informação (ENISA, 2017), o *cryptojacking* baseado em exploradores de internet (*browser-based*), funciona pela forma demonstrada no esquema da Figura n.º 5, envolvendo os quatro passos (numerados na figura), respetivamente:

1. O agente mal-intencionado (*threat actor*) compromete o seu site (ou um site terceiro);
2. Os utilizadores (*end-users*) acedem ao site comprometido e o *script* para minerar criptomoedas é executado;
3. O dispositivo com que o utilizador acedeu, começa, sem que este se aperceba, a minerar criptomoedas para a carteira digital do agente mal-intencionado;
4. Quando o dispositivo (ou o conjunto) comprometido consegue minerar um "novo bloco" na *blockchain*, o agente mal-intencionado recebe em criptomoedas, um valor correspondente a essa descoberta.

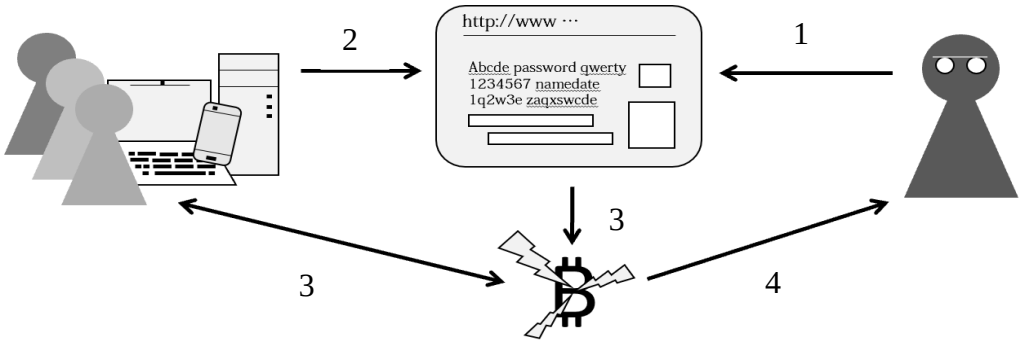

Figura n.º 5 – Esquema de funcionamento do *cryptojacking* baseado em *browsers* (ENISA, 2017).

Este processo pode ser implementado com facilidade por utilizadores comuns, nos seus domínios, visto haver diversos serviços, à semelhança do CoinHive, como o JSEcoin ou o CoinImp, que difundem todas as instruções necessárias à integração dos seus serviços *browser-based*. Posteriormente, a tática passará por atrair visitantes para o site, de modo a sustentar o sistema de mineração criado.

O excerto demonstrado na Figura n.º 6 foi reproduzido através das instruções difundidas no site oficial do serviço JSEcoin e contém as linhas de código disponibilizadas para cópia, exigindo-se apenas ao utilizador que substitua o parâmetro `<site-key>`, pela chave que lhe foi atribuída após o registo no site. É particularmente interessante denotar que, neste caso, o *script* funciona a partir de uma fonte externa (`script src`) e permite definir um limite para a utilização do processador (`throttle: X`) das máquinas de quem aceder ao site, dois fatores muito salientes para dificultar a sua deteção e atenuar os efeitos da atividade de mineração.

```
<script src="https://www.hostingcloud.racing/Adhf.js"></script>
<script>
    var miner = new Client.Anonymous('<site-key>', {throttle: 0.5});
    miner.start();
</script>
```

Figura n.º 6 – JavaScript para inserção de mineração num site (CoinImp, 2019).

Também a Cyber Threat Alliance (2018, p. 14) alerta para "recentes alterações na sofisticação da atividade ilícita de mineração", que se transcreve na personalização desenvolvida em vários níveis para aumentar as capacidades do *malware*, nomeadamente pela possibilidade de ajustar vários parâmetros relacionados com os recursos utilizados ou configurar definições com atributos que, p. ex., evitem a deteção ou cessem a mineração quando há indícios de que o utilizador está presente, através de escrita no teclado, movimentação do rato, ou outros. Em particular, o mesmo grupo indica que, ao contrário dos atacantes inexperientes, os mais avançados optam por parâmetros bastante menos detetáveis, como a utilização de apenas 20% da capacidade de processamento da CPU, reduzindo a sua taxa de mineração, em prol de conseguirem manter o seu *malware* ativo durante mais tempo nas máquinas infetadas.

No sentido de agregar e resumir alguns conteúdos recolhidos, através da Tabela n.º 2, procede-se à identificação nominal e descritiva de vários tipos de *cryptomalwares*, identificados em relatórios, artigos científicos ou por autores de referência na área da cibersegurança. As descrições apresentadas conjugam as suas visões, vincando o facto de se tratarem de *malwares* bastante flexíveis no seu modelo de atuação, adaptáveis ao ambiente em que se inserirem, alguns dotados de capacidade para dissimularem as suas funções e/ou efeitos, e quase todos com uma vasta lista de designações, o que comprova as atualizações e evoluções de que têm sido alvo, por parte de agentes mal-intencionados, sempre com o propósito de garantir que mantêm a sua volatilidade, eficácia e poder de afetação em larga escala.

Tabela n.º 2 – Designação e descrição dos *malwares* de *cryptojacking* identificados.

Designação	Descrição	Fonte
CoinHive	Partilha o nome com o serviço de mineração de Monero mais conhecido, sendo precisamente o mesmo que lhe serve de base. Pode ser introduzido maliciosamente em sites, programas ou aplicações móveis, para roubar capacidade de processamento dos dispositivos que as utilizam. Posteriormente, deu origem a diversos outros *malwares* similares.	Ioannou (2018); Check Point (2018); ENISA (2017); Newman (2017).
WebCobra	Tem origem russa e é considerado um *malware* avançado, atingindo o computador alvo sobretudo através do Windows Installer e injetando código no processo "svchost.exe". Possui o fator distinto de configurar a mineração que melhor se ajusta ao *hardware*/*software* da máquina.	Khade e Lin (2018); Wolfson (2018).
EternalMiner	Ataque que explora uma vulnerabilidade (a mesma do *ransomware* SambaCry ou EternalBlue) nos sistemas baseados em Unix, efetuando o *download* da ferramenta cpuminer (miderd) para mineração de Monero.	Check Point (2018); Kuzin *et al*. (2017).
Adylkuzz	Aproveita a mesma vulnerabilidade do *ransonware* WannaCry para se infiltrar no SO, havendo já versões modificadas e resistentes à atualização que inicialmente o inativava. Ao contrário do referido, este *malware* utiliza recursos da máquina para mineração de Monero.	Check Point (2018); Křoustek (2017); Kudo (2017); Rodrigues (2017).
WinstarNssmMiner	*Malware* baseado no serviço legítimo XMRig e que foi utilizado em meio milhão de tentativas de ataque em apenas 3 dias, através da injeção de código malicioso no processo svchost.exe em duas fases: a primeira para iniciar a mineração de Monero, a segunda para impedir a deteção e iludir as proteções de antivírus.	360 Total Security (2018); Osborne (2018).
WaterMiner	A par com o referido acima, baseia-se no serviço XMRig, podendo assumir a forma de um serviço do Windows (Winserv.exe, AudioHD.exe, Zmrig32.exe, etc.) ou ser implementado num programa (como o *mod* Arbuz para o jogo GTA V). É mais difícil de detetar do que outros, uma vez que está concebido para se desligar quando o utilizador abre o Gestor de Tarefas.	Laura (2018); Minerva Labs Research Team (2017).

Sendo o CoinHive um dos principais e mais antigos canais condutores para os *malwares* de *cryptojacking* descobertos, apesar da sua criação primária ter um propósito mais útil do que o ilícito que lhe tem sido atribuído, cabe-lhe aqui uma primeira menção, com referência aos casos de abuso que têm sido reportados. Uma das primeiras vezes que foi detetada a sua utilização deliberada, foi no conhecido site de pirataria e descarga de conteúdos ilegais Pirate Bay, onde se utilizava a capacidade de processamento dos utilizadores, sem a sua informação e consentimento. Após ter sido descoberto e tornado público o *script*, a administração do site

proferiu uma informação, para avisar que esse processo estava em fase de testes e tinha o objetivo de auxiliar a angariação de mais fundos para a manutenção daquele espaço online.

Desde então, inúmeros outros sites têm sido descobertos a correr o CoinHive, de forma oculta, e sem qualquer conhecimento por parte de quem lhes acede, inclusivamente alguns sites de renome e utilizados por milhões de internautas, tais como os blogs do Wordpress, a plataforma de comercio eletrónico Magento, vários domínios associados à plataforma de visualização de conteúdos Showtime. Quanto a estes, é importante considerar que, segundo dados citados[1], e ao contrário do que ocorreu com o Pirate Bay, dos quase 2500 sites de lojas online que foram identificados como estando infetados com este *malware*, em cerca de 85% dos casos, os lucros provenientes da mineração eram destinados apenas a duas contas do CoinHive, o que leva a crer, com elevada certeza, que o *malware* não foi colocado intencionalmente pelos proprietários dessas lojas, mas sim por terceiros que conseguiram introduzir o código malicioso. Os restantes 15%, por sua vez, destinavam-se a contas cujo nome consistia numa *tag* indicativa do site ao qual estavam associadas, pelo que, supõe-se, possa representar um atacante único (ENISA, 2017).

São igualmente preocupantes, os casos de sites fidedignos, mas que incorporam JavaScripts ativos de terceiros, introduzidos com vários fins, como a publicidade, as ferramentas de acessibilidade, os serviços de análise de tráfego ou o rastreamento de acessos. Os privilégios concedidos a terceiros, para introdução desses conteúdos, materializam a possibilidade dos próprios, ou de outros agentes por intermédio de quebras de segurança, injetarem *scripts* de *cryptojacking*. Sendo os alvos mais remuneradores destes *malwares* os sites com visitas de maior duração, há registos de incidentes em que o *script* do CoinHive, através do Google Tag Manager, foi inserido nos sites da Movistar e da Globovision, bem como há registos da sua presença, durante cerca de uma semana, em anúncios do YouTube mostrados aos utilizadores de vários países, como França e Japão (Eskandari *et al.*, 2018).

Para além dos conteúdos presentes no próprios sites, foram ainda detetados comprometimentos através da instalação de extensões, *addons* ou *plugins* nos exploradores de internet, de que é exemplo o Short URL (`goo.gl`)[2], destinado a criar um URL abreviado para os sites visitados no Google Chrome e retirado diretamente da sua loja oficial, que em outubro de 2017 contava com mais de 14000 utilizadores (representando um potencial lucro bastante significativo) e tinha uma avaliação de 4.5 (de 1 a 5), proveniente de quase 90 pessoas, o que significa que, aparentemente, ninguém desconfiou do que se passava no plano de fundo dessa aplicação. A sua atuação, no caso concreto, envolvia a transferência de um ficheiro chamado cryptonight.wasm do site do CoinHive, de 10 em 10 segundos, provocando o aumento da utilização do CPU para 95%, para mineração da criptomoeda Monero (ENISA, 2017). Por outro lado, existem também extensões para o Chrome, como a NoCoin, que bloqueiam a abertura de sites com *scripts* do CoinHive ativos (Newman, 2017).

[1] Fonte: `https://gwillem.gitlab.io/2017/11/07/cryptojacking-found-on-2496-stores`, acedido em 2019/01/23.

[2] Fonte: `https://medium.com/@ale_polidori/with-this-article-i-would-like-to-share-a-real-experience-of-discovering-a-malware-that-mines-36e26c8dfe1e`, acedido em 2019/01/23.

Por fim, há menção a outros esquemas, incluindo falsas atualizações de Java[3], variantes de *cryptojacking* em aplicações para Android[4], tentativas de replicação de domínios conhecidos[5] (como o `www.twiter.com.com`), esquemas de publicidade ou suporte técnico enganosos[6] (contendo redireccionamentos não fidedignos), exploração de fragilidades em serviços de armazenamento na nuvem[7] (p. ex., no Google Cloud Plataform, Azure e AWS) e o surgimento de variações do CoinHive e outros similares[8] (como o CoinNebula), motivadas pelo sucesso conseguido nos primeiros ataques (ENISA, 2017).

Num esforço para contenção destes *malwares*, concebidos para dar lucro aos seus exploradores e vários prejuízos às vítimas, a US-CERT (2018) deixa várias advertências de boas práticas para uma prevenção eficaz na defesa contra o *cryptojacking*, tais como:

- Utilizar *software* de antivírus, que irá proteger o sistema contra as ameaças de *malware* já detetadas e reconhecidas, permitindo ao utilizador remover qualquer programa indesejado antes que seja provocado qualquer dano;
- Utilizar *firewall*, que poderá auxiliar a prevenir e mitigar alguns vetores de ataque, através do bloqueio do tráfego de dados maliciosos, antes destes poderem atingir o sistema computacional;
- Manter o SO e restante *software* atualizados, para que os atacantes não possam retirar vantagem de vulnerabilidades publicamente conhecidas;
- Criar palavras-passe fortes, não abdicando de alterar as pré-definidas, uma vez que essas, frequentemente, estão disponíveis para quem as quiser pesquisar ou através de geradores de chaves;
- Verificar as políticas de privilégios do sistema, passando prioritariamente por garantir que os utilizadores com permissões de administrador possuem efetivamente essa necessidade, e que os restantes estão limitados somente às funções que lhes competem;
- Aplicar filtros de aplicações, normalmente designado por *whitelisting*, de modo a prevenir que código malicioso ou ficheiros executáveis sejam iniciados autonomamente;
- Ter especial cautela com os *downloads* de ficheiros feitos a partir de sites desconhecidos ou não confiáveis, devendo procurar sempre a fonte de origem legítima, para as transferências da internet;
- Aprender a reconhecer atividade normal e anormal da CPU, bem como das restantes componentes do sistema, para facilitar a sua monitorização e permitir a reação imediata face a qualquer atividade suspeita ou degradação repentina e injustificada de desempenho;

[3] Fonte: `https://twitter.com/malwrhunterteam/status/911644745608433664`, acedido em 2019/01/24.
[4] Fonte: `https://twitter.com/virqdroid/status/925336630948454400`, acedido em 2019/01/24.
[5] Fonte: `https://www.bleepingcomputer.com/news/security/coinhive-is-rapidly-becoming-a-favorite-tool-among-malware-devs`, acedido em 2019/01/24.
[6] Fonte: `https://blog.trendmicro.com/trendlabs-security-intelligence/eitest-campaign-uses-tech-support-scams-deliver-coinhives-monero-miner`, acedido em 2019/01/23.
[7] Fonte: `https://www.theregister.co.uk/2017/10/17/cryptocoin_miners_turning_up_on_unprotected_cloud_instances`, acedido em 2019/01/24.
[8] Fonte: `https://twitter.com/WDSecurity/status/919831580184645632`, acedido em 2019/01/24.

- Desativar/desinstalar os serviços, programas ou aplicações que não são utilizados nem necessários, de forma a descongestionar o sistema, conhecer os seus constituintes e ainda para eliminar *software* potencialmente lesivo para o utilizador e que, por vezes, vem previamente integrado nos próprios sistemas (*toolbars*, temas, jogos e outro *adware* não essencial);
- Validar os *inputs*, que se constitui como uma medida para amenizar os ataques por *injection* (injeção de código malicioso), nos quais o *cryptojacking browser-based* se fundamenta, podendo p. ex., desativar a execução automática de conteúdos JavaScript nos *browsers*;
- Criar e controlar *blacklists*, sobretudo com base em fontes credíveis e relatórios de segurança, que sejam reconhecidos por monitorizar sites da internet, em busca de atividades suspeitas e maliciosas, para poder preveni-las e bloqueá-las.

A propósito do que foi referido até ao momento, e atentando à discussão do artigo de Eskandari *et al.* (2018), há uma questão pouco abordada e deveras interessante, que se prende com a possibilidade de utilização de alguns dos códigos e *scripts* mencionados para mineração de criptomoedas de forma legal, através de determinados sites. Numa situação em que o site informe e alerte o utilizador para a atividade de mineração que ocorrerá durante o período em que se encontre a visitar a página, poderá considerar-se que não há prática ilícita? A hipótese é discutível, uma vez que o cidadão comum não possui, ainda, conhecimento adequado que o permita aceitar essa opção, tomando consciência das envolventes na sua plenitude. Ainda assim, julga-se que a possibilidade de aceitar o aproveitamento de recursos do sistema de terceiros, nomeadamente de processamento, informando devidamente e para fins lucrativos, é discricionária de cada utilizador, tal como ocorre com a aceitação do registo de *tracking* ou com a utilização de *cookies*, quando se abrem determinados sites.

Um dos casos típicos desta situação, que até se poderia constituir como um novo modelo de negócio, seria a justificação, nos sites, de que é mais conveniente ao utilizador e ao próprio serviço, ao invés de apresentar inúmeras publicidades (frequentemente indesejadas por quem as visualiza), aproveitar uma parte da capacidade de processamento (e, consequentemente, da energia) do utilizador para minerar, gerando lucro e recompensando o trabalho e as despesas na manutenção dos serviços prestados, tais como os de agências noticiosas ou os de transmissão de conteúdos musicais/cinematográficos (Rodriguez e Posegga, 2018).

No que confere a esta parte, é interessante mencionar que o primeiro caso de responsabilização legal relacionado com *cryptojacking*, deu-se em julho de 2018, no Japão, condenando um jovem de 24 anos por ter obtido lucro equivalente a 45 dólares, proveniente de uma "*online gaming cheat tool*", que disponibilizou no seu blog e que executava mineração ilícita de Monero (com base no CoinHive) no *background* dos utilizadores da ferramenta (Osborne, 2018a).

Capítulo 3

Metodologia

Pretendendo-se estabelecer o pleno sentido e compreensão entre ambas as partes do trabalho, apresenta-se seguidamente, na Figura n.º 7, o modelo metodológico completo, integrando as matérias e os propósitos de pesquisa decorridos do estudo teórico, bem como a sequência que se propõe cumprir para a realização da parte prática, correspondente ao estudo da influência de *cryptojacking* nos recursos de processamento dos sistemas. Todos os componentes do modelo contêm derivações ou interligações, o que exige que seja ponderado o caminho percorrido em várias fases do processo e que todo o trabalho culmine com a resposta às questões intrínsecas, assinalando-se, por fim, as conclusões e elaboração de propostas para análises futuras.

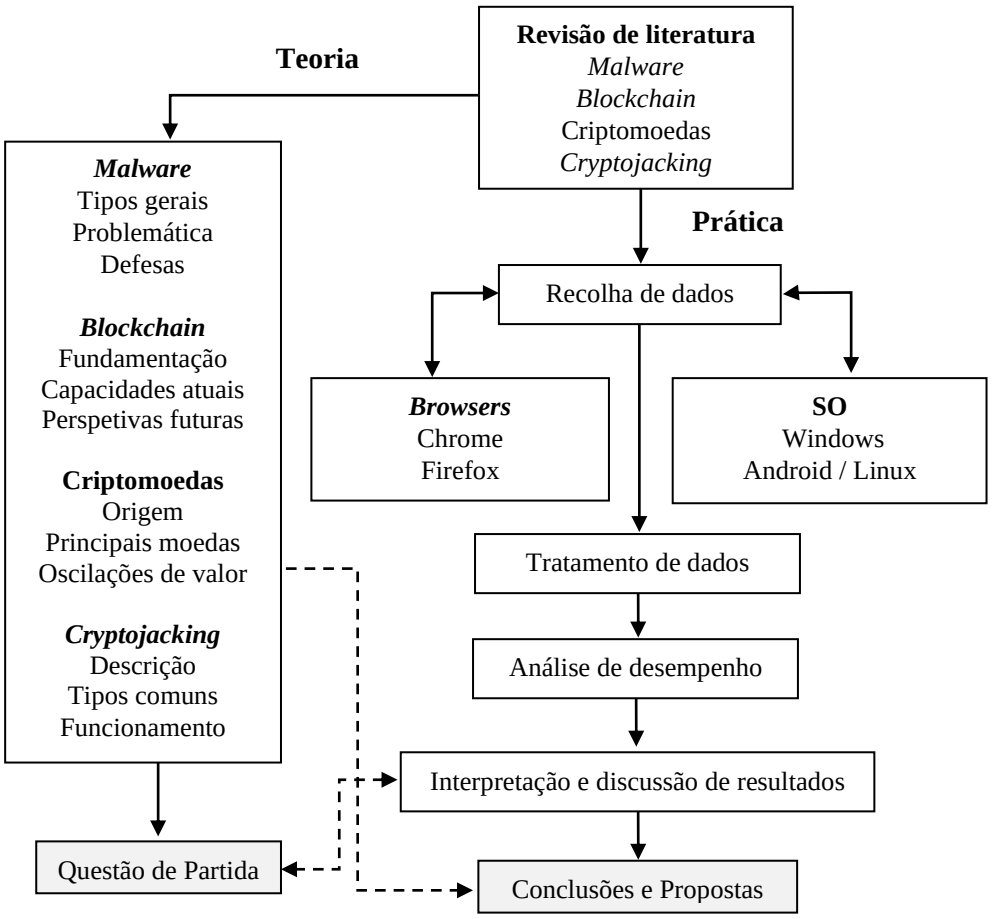

Figura n.º 7 – Modelo metodológico.

Para concretizar a parte prática do presente estudo e cumprir o objetivo de aferir quais as influências dos *malwares* de *cryptojacking* no desempenho de diferentes sistemas, é necessário primeiramente selecionar algumas propriedades para equilibrar as medições e o respetivo impacto na utilização. Nesse sentido, e por praticabilidade, optou-se por utilizar a mesma máquina física para todos os testes – um computador portátil, de marca Microsoft, modelo Surface Pro de 5.ª geração, com as seguintes caraterísticas técnicas principais (Microsoft, 2019):

- SO – Windows 10 Pro;
- Armazenamento – *Solid State Drive* (SSD) com 256 Gigabytes (GB) de capacidade;
- Processador (CPU) – Intel® Core™ i5-7300U @ 2.60Ghz / 2.71Ghz;
- Gráficos (GPU) – Intel® HD Graphics 620 (integrada) com 128MB dedicados;
- Memória – 8GB RAM;
- Acessórios – Teclado Microsoft com *touchpad* integrado.

O processo de análise de *software* pode efetuar-se de forma estática ou dinâmica. A primeira é realizada sem execução, empregando-se exclusivamente pela inspeção do código-fonte, por representações binárias dos programas ou pelo cálculo matemático de valores possíveis para os vários parâmetros. Por sua vez, a menos limitada análise dinâmica aplica-se durante a execução dos programas e pode consumar-se por várias formas, tais como: a análise em modo kernel, que permite ao investigador "esconder" a sua atividade de análise perante *malwares* que só se executem em modo de utilizador normal, possibilitando a aquisição de informações adicionais do sistema; a análise através de emulação de componentes ou sistemas completos, permitindo, consoante os parâmetros definidos, obter uma *sandbox* (ambiente virtualmente seguro e que quebra o contacto com o domínio em que se insere), eficaz para o investigador controlar e analisar todos os aspetos de execução de um programa, enquanto corre código potencialmente malicioso, sem temer os impactos negativos no sistema real; e a análise em máquina virtual (MV), traduzindo-se pela virtualização de componentes de *hardware* de um sistema físico base, para simular um sistema isolado e com os privilégios e parâmetros pretendidos para determinado fim (Egel *et al.*, 2012).

Sanabria (2007) afirma que as MV são ferramentas esplêndidas para investigadores de *malware*, identificando como vantagens, o baixo custo de implementação (quando comparado com a aquisição de máquinas para testes ou a montagem de um laboratório dedicado), a flexibilidade (conferindo a possibilidade de restaurar uma máquina ao seu estado inicial com grande facilidade e em pouco tempo) e a capacidade de isolamento da rede, quando necessária. Como desvantagem, é apontada a crescente probabilidade do *malware* ter sido desenvolvido já com o propósito de evitar ambientes de virtualização, podendo impedir o seu estudo por não se manifestar de todo, ou por apresentar comportamentos diversos.

Seguindo a linha condutora para concretizar análises dinâmicas, e considerando a afirmação de Goldberg (*cit in* Egel *et al*., 2012, p. 14), de que uma MV é "uma duplicação eficiente e isolada de uma máquina real", para efetuar os testes propostos em ambiente

seguro, controlado e equiparado, criaram-se MV no referido computador portátil, que se manterá ligado à corrente e em modo de desempenho máximo durante todo o processo.

Surge neste momento a necessidade de refletir sobre outras duas questões:

- É preferível criar MV que tenham acesso a todos os recursos (cores e potência) de processamento do computador, ou será mais cauteloso limitar o acesso a uma parte do seu poder total, para salvaguardar o sistema original?
- Para uma eficaz medição de desempenho, deverá fazer-se a monitorização através de programas adequados a cada SO dentro da própria MV, ou poderá fazer-se essa análise monitorizando a partir do sistema original?

Partindo do princípio que, se não fosse incauto e inseguro, a experiência seria realizada numa máquina real, a ponderação tendeu a agrupar estas perguntas, considerando-se que a forma mais realista e que permitirá melhor equiparação de resultados, é a atribuição do poder de processamento máximo à MV, permitindo que a monitorização seja executada com autenticidade a partir do seu exterior, pois a MV estará a utilizar os mesmos recursos de processamento (CPU e GPU) que o sistema original.

Para a concretização do capítulo seguinte, foi adotado um esquema de trabalho, que contempla todas as cinco etapas a cumprir na parte prática, encontrando-se abaixo representado na Figura n.º 8.

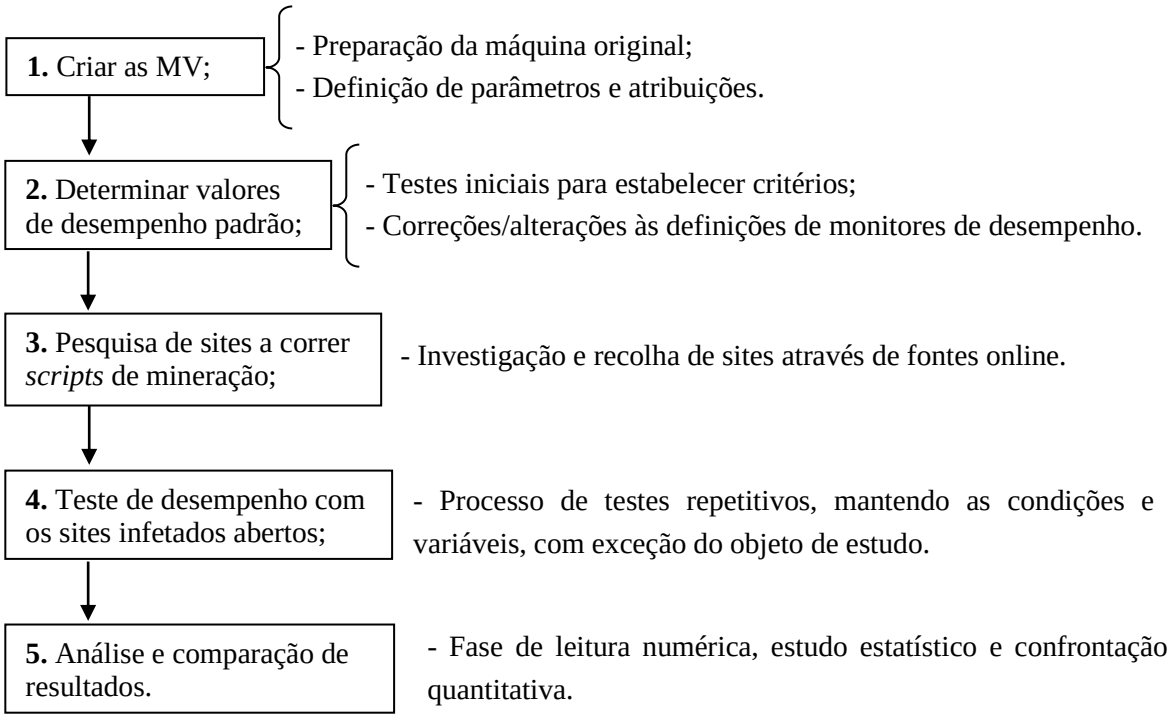

Figura n.º 8 – Esquema de trabalho prático.

Capítulo 4

Influência do *cryptojacking* no desempenho

Visa-se agora aferir, de forma prática, se o *cryptojacking* provoca, tal como apreendido na parte teórica, alterações ao desempenho dos sistemas afetados.

A experiência, terá o seu fundamento na seleção de uma lista de sites, que sejam identificados como contendo *scripts* de *cryptojacking* no seu código, procedendo-se, posteriormente, à execução de vários testes a cada site, em ambientes diversificados, para comprovar se os efeitos no desempenho, provocados pela abertura desses sites, se coadunam com o espectável para uma atividade de mineração ativa.

Com esse fim, subdivide-se o presente capítulo em várias fases, começando-se por expor os detalhes relativos à amostra constituída e aos valores que vão servir como termo de comparação, abordando-se depois os indicadores de *cryptojacking*, e terminando com a análise particular aos resultados obtidos.

4.1. Amostra e valores de referência

No cumprimento dos pressupostos definidos pela metodologia e pelo esquema, ambos indicados no capítulo anterior, compete agora dar início à parte experimental, que começa obrigatoriamente com a determinação dos valores padrão para o desempenho da máquina.

Partiu-se então para a criação de três MV, com auxílio do programa Oracle VirtualBox (versão 5.2.26 128414), para correr três SO diferentes. Pelas caraterísticas e necessidades específicas para correr os SO selecionados em MV, atribuíram-se 3GB, dos 8GB de memória RAM disponíveis, definindo-se propriedades diferentes apenas no que concerne ao tipo e capacidade de armazenamento dos discos virtuais.

Para evitar a utilização de ferramentas de medição de desempenho que pudessem interagir de forma diferente com as propriedades das MV criadas, tal como para efeitos de normalização na recolha de dados, foi escolhido o Monitor de Desempenho (MD) nativo do Windows 10, para recolha dos dados relativos às percentagens de utilização da CPU e da GPU, assim como para o registo das velocidades de transferência (dados recebidos e enviados) registados na placa de rede. Por não ser possível medir a temperatura de sensores térmicos digitais, através do MD, para efetuar essa tarefa escolheu-se o CoreTemp (versão 1.13), programa disponível online para transferência gratuita.

Na fase seguinte, para reunir sites (alegadamente) infetados para testar, observaram-se os estudos de Eskandari *et al.* (2017), de dezembro de 2017, e de Mursch (2018), de fevereiro de 2018, que conduziram experiências semelhantes para tentar descobrir as quantidades de *malware* de *cryptojacking* existentes à data. Os investigadores pesquisaram pelos *scripts* através do site `www.publicwww.com`, que se constitui como uma ferramenta para descoberta de fragmentos alfanuméricos, assinaturas, expressões-chave ou palavras em mais de 500 milhões de páginas online que utilizem código HTML, JavaScript e CSS.

Da mesma forma, para o presente experimento, recorreu-se ao site `www.publicwww.com`, efetuando-se a pesquisa inicial através de *strings* relacionadas com os referidos *scripts*, na mesma linha procedimental que os autores citados acima adotaram. Para esse efeito, começou por introduzir-se, no motor de busca, o nome pelo qual o *script* é conhecido, repetindo-se a pesquisa quando se obtiveram expressões mais precisas, como p. ex., os parâmetros reais dos *scripts*, conforme se indica nos pontos em baixo:

- CoinHive – coinhive.min.js e coinhive.anonymous;
- Crypto-Loot – cryptoloot.pro, crypto-loot.com e cryptoloot.anonymous;
- CoinImp – hostingcould.racing e hashing.win;
- deepMiner – deepminer.anonymous e deepminer.min.js;
- JSEcoin – load.jsecoin.

Como resultado, a Tabela n.º 3 agrega os cinco tipos de *cryptojacking* em que se concentra esta parte prática e sobre os quais se pesquisaram as respetivas *strings* e domínios, apresentando-se também, nos conteúdos da tabela, a criptomoeda principal minerada por cada um deles e, nas últimas colunas, os resultados para comparação, entre os valores unitários das criptomoedas e o número de sites encontrados, quer pelas experiências de Eskandari *et al.* (2017) e de Mursch (2018), quer pela que se realiza no presente trabalho.

Tabela n.º 3 – Resultados gerais para pesquisa de *cryptojacking*.

Designação	Criptomoeda principal minerada	Valor unitário			N.º sites encontrados		
		Eskandari *et al.* (2017)	Mursch (2018)	Atual[9]	Eskandari *et al.* (2017)	Mursch (2018)	Atual[10]
CoinHive	XMR	~260€	~200€	~60€	30.611	34.474	15.385
Crypto-Loot					695	2.057	319
CoinImp					317	4.119	989
deepMiner					n.d.	2.160	2.258
JSEcoin	JSE	desc.	desc.	~0,0006€	1.131	n.d.	1.841

Legenda: ~ – Valor aproximado; **n.d. –** Quantidade não disponível, por não se ter contemplado essa criptomoeda na experiência; **desc. –** Desconhecido, por falta de histórico de valores fidedigno.

[9] Valor de uma unidade da criptomoeda correspondente, em Euros, com fonte em `https://www.worldcoinindex.com/pt/Moeda`, acedido em 2019/04/30.

[10] Número total de sites onde as *strings* pesquisadas se encontram presentes, com fonte em `https://publicwww.com/websites`, acedido em 2019/04/30.

Pela análise à Tabela n.º 3, verifica-se que, em comparação geral entre os vários resultados, o número de sites encontrados com indícios de presença de *malware* de mineração no seu código fonte, teve o seu pico na listagem obtida pelo trabalho de Mursch (2018). Isso poderá dever-se a vários fatores, tais como: as pesquisas no Publicwww, terem sido elaboradas com recurso à introdução de *strings* diferentes, havendo a real possibilidade de que nem todas elas resultem no mesmo número de resultados; a clara valorização do Monero (Figura n.º 3), entre o fim de 2017 e inicio de 2018, aumentando a rentabilidade da mineração; ou, para justificar o mais recente acontecimento de encerramento do serviço oficial do CoinHive, em março do presente ano, reduzindo drasticamente o número de sites a correr o seu *script*, por este alegadamente já não se encontrar ativo.

Visualiza-se também, pela tabela, que a quantidade de sites encontrados, atualmente, com o deepMiner, é semelhante à de 2018, e que, comparativamente a 2017, a presença do JSEcoin subiu razoavelmente. Estes resultados poderão estar relacionados com a procura de alternativas sustentáveis, face aos serviços que foram desativados.

Para iniciar a fase de testes e medir os efeitos do *cryptojacking*, de todos os registos encontrados através do site `www.publicwww.com`, selecionou-se aleatoriamente uma amostra de 20 sites de cada tipo (CoinHive, Crypto-Loot, CoinImp, deepMiner e JSEcoin), substituindo-se, de forma igualmente aleatória, os sites que não abriram na execução do primeiro teste, totalizando uma amostra de 100 sites.

Ao acima descrito, e como complemento aos resultados obtidos pelo Publicwww, acrescentou-se também a pesquisa pelos sites selecionados, desta feita, através de dois outros sites (`www.notmining.org` e `www.wappalyzer.com`), o que permitiu aferir se, para além de existirem elementos de mineração nas suas linhas de código, teriam outros indicadores que comprovassem se esses elementos estavam presentes e em funcionamento.

No primeiro caso, o Notmining**,** auxiliou a verificar a existência de *scripts* de mineração ativos nos elementos constituintes dos sites analisados. O segundo, Wappalyzer, trata-se de uma plataforma com capacidade para detetar e identificar mais de 1.000 tecnologias utilizadas em sites, filtrando os conteúdos por categorias, como p. ex., JavaScript (Frameworks, Graphics ou Libraries), Reverse Proxy ou Cryptominer. Dentro desta última categoria, o Wappalyzer reconhece 14 estirpes, que podem estar agregadas ao código fonte dos sites, sendo elas: CoinHive, CoinHive Captcha, Coinhave, Cloudcoins, CoinImp, Coinlab, Crypto-Loot, deepMiner, Inwemo, JSEcoin, Minero.cc, Monerominer, ProjectPoi e Webmine (Wappalyzer, 2019).

A cada site da amostra foi atribuído um número de identificação (entre 1 e 100), para facilitar a sua menção ao longo do trabalho, podendo visualizar-se a listagem completa dos sites da amostra, bem como as plataformas que identificaram cada site, na Tabela n.º 8 do Apêndice A.

Durante a execução dos testes, a máquina original manteve-se a correr apenas os serviços essenciais ao funcionamento do sistema, permaneceu localizada no mesmo espaço físico, não foi sujeita a oscilações significativas da temperatura ambiente, salvaguardando-se, deste modo, a manutenção das condições da experiência. Nas MV, abriu-se apenas uma

instância e um separador do *browser* em teste, no site a ser testado. A monitorização iniciou-se logo após o carregamento dos sites estar concluído e teve a duração de três minutos, durante os quais não houve qualquer atividade da parte do utilizador, mantendo-se apenas a página inicial aberta.

Foram desligadas todas as atualizações automáticas, quer na máquina original, quer nas MV, com a finalidade de não influenciar a medição da velocidade de transferência. De igual modo, para que as ferramentas de monitorização retornassem aos valores padrão, para garantir que a temperatura voltava ao normal e para analisar qualquer potencial efeito secundário não referenciado, entre cada teste, aguardou-se inativamente, pelo menos, durante o período de três minutos.

Deste modo, e no seguimento do modelo metodológico apresentado no capítulo anterior, realizaram-se quatro testes para cada um dos 100 sites selecionados para amostra, decorrendo, cada teste, num ambiente diferente – Windows e Chrome / Windows e Firefox / Android (através de MV no Windows) e Chrome / Linux (através de MV no Windows) e Firefox – de forma a poder recolher resultados dos vários SO e *browsers* utilizados.

Por sua vez, durante a execução de cada teste, foram registados os valores de oito variáveis, respetivamente:

- $\%CPU_{máx}$ – Percentagem máxima de utilização da CPU;
- $\%CPU_{mín}$ – Percentagem mínima de utilização da CPU;
- $\%CPU_{m}$ – Percentagem média de utilização da CPU;
- $\%GPU_{máx}$ – Percentagem máxima de utilização da GPU;
- $\%GPU_{mín}$ – Percentagem mínima de utilização da GPU;
- $\%GPU_{m}$ – Percentagem média de utilização da GPU;
- Tf_{c} – Temperatura final da CPU, em graus Celcius;
- v_{m} – Velocidade média de envio e receção, da placa de rede, em Kilobits (Kbit) por segundo.

Para obtenção de alguns valores referenciais, que servissem de modelo e fossem prévios aos testes à amostra, executaram-se os quatro testes, nas condições referidas à priori, a alguns sites conhecidos e de acesso livre.

A Tabela n.º 4 agrega os registos provenientes dos testes a estes cinco sites selecionados para referência, tendo sido, cada teste, realizado dentro dos ambientes já referidos (SO e *browsers* diferentes), incluindo-se ainda os resultados médios (dos quatro testes) para cada um destes sites. Salienta-se que, os cinco sites, são dotados de caraterísticas díspares, ao nível de visual, multimédia e quantidade e especificidade dos *scripts* carregados, conforme se determina:

- R1 – `www.google.com`;
- R2 – `www.facebook.com`;
- R3 – `www.youtube.com`;
- R4 – `www.ebay.com`;
- R5 – `www.sapo.pt`.

Tabela n.º 4 – Valores de referência obtidos para os testes a cinco sites comuns, distribuídos por *browser* e por SO.

N.º	*Browser*	SO	%CPU máx	%CPU mín	%CPU m	%GPU máx	%GPU mín	%GPU m	Tf_c	v_m
R1	Chrome	W	16,21	**2,06**	5,54	1,08	0,30	0,48	**40,00**	2,80
		A	11,72	0,43	4,24	1,19	0,18	0,29	38,00	4,71
	Firefox	W	**22,38**	1,67	**6,30**	**1,54**	**0,41**	**0,74**	**40,00**	1,59
		L	13,66	1,15	4,67	1,39	0,16	0,33	37,00	**4,86**
	Média		15,99	1,33	5,19	1,30	0,26	0,46	38,75	3,49
R2	Chrome	W	12,61	0,00	4,41	3,06	0,17	0,33	**43,00**	1,82
		A	38,93	**4,32**	**9,30**	**9,79**	**0,70**	**1,12**	39,50	4,55
	Firefox	W	37,59	2,63	6,58	1,21	0,38	0,64	40,00	6,39
		L	**53,97**	0,61	5,99	1,81	0,17	0,41	42,00	**13,65**
	Média		35,78	1,89	6,57	3,97	0,36	0,63	41,13	6,60
R3	Chrome	W	31,34	0,24	3,68	1,56	0,16	0,31	39,00	26,16
		A	**46,56**	**1,24**	**5,81**	4,26	**0,17**	0,36	40,50	5,80
	Firefox	W	40,37	0,00	4,64	**5,15**	**0,17**	**0,37**	41,00	**28,03**
		L	39,54	0,86	5,50	2,10	0,16	0,28	**41,50**	10,18
	Média		39,45	0,59	4,91	3,27	0,17	0,33	40,50	17,54
R4	Chrome	W	**68,82**	0,52	9,49	5,45	0,17	0,84	42,00	5,58
		A	53,19	**1,81**	**15,91**	4,03	**0,18**	**1,33**	43,50	**18,72**
	Firefox	W	49,29	0,00	6,64	6,65	0,17	0,84	40,00	8,48
		L	32,53	0,04	10,56	**6,99**	**0,18**	0,75	**46,00**	6,70
	Média		50,96	0,59	10,65	5,78	0,18	0,94	42,88	9,87
R5	Chrome	W	**81,76**	0,82	5,40	2,56	0,09	0,33	38,50	25,24
		A	68,79	1,13	**6,32**	**5,25**	**0,18**	**0,41**	**42,00**	**65,42**
	Firefox	W	25,13	0,00	3,36	3,46	0,17	0,38	40,50	4,30
		L	58,26	**1,44**	6,08	2,08	0,17	0,32	38,00	41,07
	Média		58,49	0,85	5,29	3,34	0,15	0,36	39,75	34,01

Legenda: "Negrito" – Valor mais elevado registado para a variável, por site; **R1 –** `www.google.com`; **R2 –** `www.facebook.com`; **R3 –** `www.youtube.com`; **R4 –** `www.ebay.com`; **R5 –** `www.sapo.pt`; **W –** Windows; **A –** Android; **L –** Linux.

Os valores recolhidos pelos testes de referência constatam um padrão natural para o desempenho de um computador que acede, através de um *browser*, a um site (página inicial, apenas) que não contém *malware* de mineração embutido no seu código. Verificam-se registos máximos da utilização da CPU entre os 16 e 58% e mínimos entre 0 e 7%, médias de utilização da CPU entre 5 e 11%, máximos de utilização da GPU entre 1 e 6% e mínimos todos a rondar os 0%, médias de utilização da GPU entre 0 e 1%, temperaturas finais entre 39 e 43ºC e velocidades médias de transferências de dados entre 3 e 34 Kbit/s. Estes são os valores que servirão posteriormente para confrontação de resultados.

4.2. Indicadores de *cryptojacking*

Os quatro testes, realizados a cada um dos 100 sites da amostra (identificados, através das plataformas, como estando a minerar), tiveram a duração total de, aproximadamente, 45 horas. Correu-se, assim, um conjunto de 400 testes (de referir que, em seis dos quais, não foi possível recolher resultados, por motivo do site ter deixado de estar disponível), nos vários SO – 200 testes no Windows, 100 testes no Android e 100 testes no Linux. Quanto aos *browsers*, no Windows utilizou-se o Chrome e o Firefox, no Android utilizou-se o Chrome e no Linux usou-se o Firefox, permitindo, deste modo que houvesse sempre um termo de comparação, dentro e fora de cada SO e *browser*. Ao longo desta parte experimental foram recolhidos um total de 3.360 dados, reunidos em bruto na Tabela n.º 9 do Apêndice B.

Uma vez que não foi possível encontrar, pela revisão bibliográfica, resultados padrão para este tipo de testes, derivado da falta de experiências nesta área, e dado que, a existirem e estarem ativos, os *scripts* de mineração podem estar definidos dentro de parâmetros menos detetáveis ao utilizador, como aliás foi referido na parte teórica, ponderaram-se alguns valores razoáveis para aferir se os sites da amostra conteriam mesmo *malware* de mineração, ou não, com base nas duas variáveis mais referidas por diversas fontes bibliográficas – percentagem de utilização da CPU e respetiva temperatura atingida. Assim, e dado que, nem todos os sites da amostra se enquadraram no mesmo espectro de resultados, ou seja, houve sites que, notoriamente, não desencadearam sintomas anormais que se relacionassem com as variáveis em teste (por estarem, p. ex., com o *malware* de mineração inativo), surgiu a necessidade de determinar critérios de designação.

Para tal, averiguou-se a distribuição quantitativa, por intervalos, dos valores obtidos para as duas variáveis mencionadas, concluindo-se que, conforme se observa na Figura n.º 9, os resultados obtidos para a percentagem de utilização média da CPU, agrupam-se, essencialmente, até aos 20%, distinguindo-se os sites cujos testes atingiram, ou excederam, esse valor. Em termos percentuais, constata-se que, em apenas 22% dos testes, o valor da percentagem média de utilização da CPU foi igual, ou superior, a 20%. Destaca-se, em especial, os 40 casos (representando 10% do total dos testes), em que a percentagem média de utilização da CPU igualou, ou superou, os 40%.

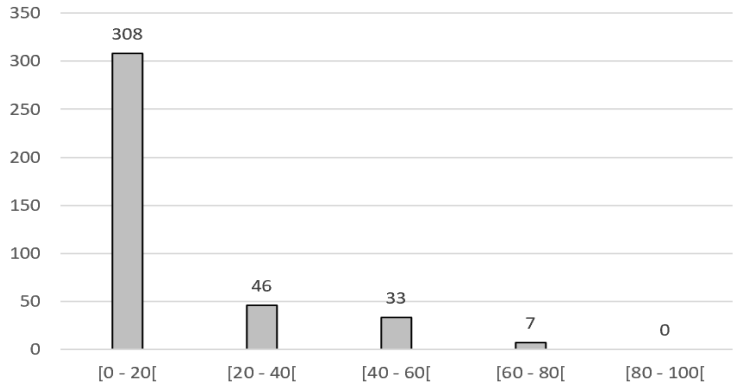

Figura n.º 9 – Histograma da percentagem média de utilização da CPU ($\%CPU_m$).

E, tal como se extrai da Figura n.º 10, nos resultados alcançados para a temperatura registada no final de cada teste, verifica-se uma incidência bastante mais elevada no intervalo de valores entre 25ºC e 50ºC. Assim, destacam-se do conjunto, os sites cujo final dos testes igualou, ou superou, a temperatura de 50ºC.

Verifica-se ainda que, estatisticamente, a temperatura de 50ºC só foi igualada, ou ultrapassada, em 28% dos testes, com destaque particular para os dois sites (que representam somente 0,005% do total dos testes), em que a temperatura de 75ºC foi atingida ou superada.

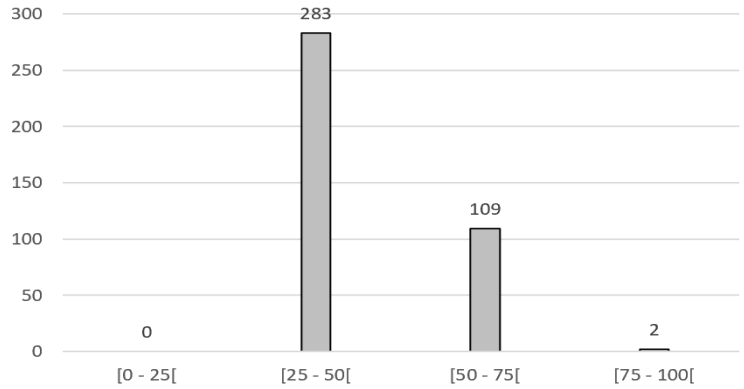

Figura n.º 10 – Histograma da temperatura registada no final de cada teste, em graus Celsius (Tf_c).

Tendo-se analisado atentamente os resultados dos testes aos sites de referência, os resultados dos testes aos 100 sites da amostra, e não esquecendo o que é descrito na parte teórica, nomeadamente, no que concerne aos efeitos provocados pela mineração, cabe, neste momento, afirmar que é necessário enquadrar os resultados obtidos, assumindo-se a possibilidade de, apesar da amostra ter sido obtida com base na pesquisa por *scripts* que se relacionassem com *cryptojacking*, nem todos os sites tenham código de mineração efetivamente em execução.

Perante o que se observa, efetuou-se a divisão dos cinco sites de referência (que não contêm *scripts* de mineração) e dos 100 sites da amostra (que, alegadamente, continham indicadores de mineração), por quatro categorias, duas das quais dentro dos resultados considerados negativos para *cryptojacking*, e outras duas, dentro dos resultados considerados positivos.

Para os sites da amostra, a divisão assenta nos resultados obtidos pelos quatro testes efetuados a cada um deles, com o intuito de separar os casos em que se considera improvável a presença de mineração (não significando que esta não existiu, apenas que não foi verificada pelos resultados dos testes), os casos em que há possibilidade de existir essa atividade (por se manifestar no desempenho, em alguns dos testes realizados a esses sites) e os casos em que essa atividade foi notória (por se manifestar no desempenho da maioria dos testes efetuados a esses sites). Portanto, dentro dos sites que se designaram como sendo "positivos", a única diferença assinalada para classificação dentro da categoria de "indiciado" ou "comprovado", foi o número de testes (dentro dos quatro efetuados) que apresentou resultados que se enquadram explicitamente na atividade de mineração, consoante a categorização que se segue.

Nos pressupostos indicados, dividem-se os resultados enquanto negativos, ou positivos, para *cryptojacking*. Atendendo aos 420 testes executados a um total de 105 sites selecionados, a categorização e respetivo quantitativo ocorrem com fundamento nas seguintes premissas:

- Resultados negativos:
  - **Referência** – 5 sites selecionados para referência e comparação (não integram a amostra), por se considerarem legítimos, díspares entre si, e não conterem *scripts* de mineração no seu código fonte;
  - **Livres** – 42 sites da amostra, que aparentam estar livres de *cryptojacking*, por não ostentarem atividade de mineração ativa, dado os seus resultados serem, em tudo, semelhantes aos dos sites de referência, não se enquadrando, portanto, nas conjeturas mínimas definidas para as categorias de "resultados positivos".
- Resultados positivos:
  - **Indiciados** – 40 sites da amostra, que aparentam ter atividade de mineração ativa, enquadrando-se nesta categoria todos os que, em um ou dois dos quatro testes realizados, originaram uma percentagem média de utilização da CPU igual, ou superior, a 20% e/ou geraram uma temperatura final da CPU igual, ou superior, a 50ºC;
  - **Comprovados** – 18 sites da amostra, que apresentam uma notória atividade de mineração, enquadrando-se nesta categoria todos os que, em pelo menos três, dos quatro testes realizados, originaram uma percentagem média de utilização da CPU igual, ou superior, a 20% e/ou geraram uma temperatura final da CPU igual, ou superior, a 50ºC.

Desta forma, surgem as três categorias que, adiante, se utilizam para comparação de resultados – sites de referência (negativos), sites indiciados (positivos) e sites comprovados (positivos), com especial enfoque nestas últimas duas categorias.

Verifiquem-se as Figuras n.º 11, 12 e 13, para visualização dos gráficos de desempenho tipicamente obtidos, respetivamente para os testes aos sites de referência, aos sites indiciados e aos sites comprovados.

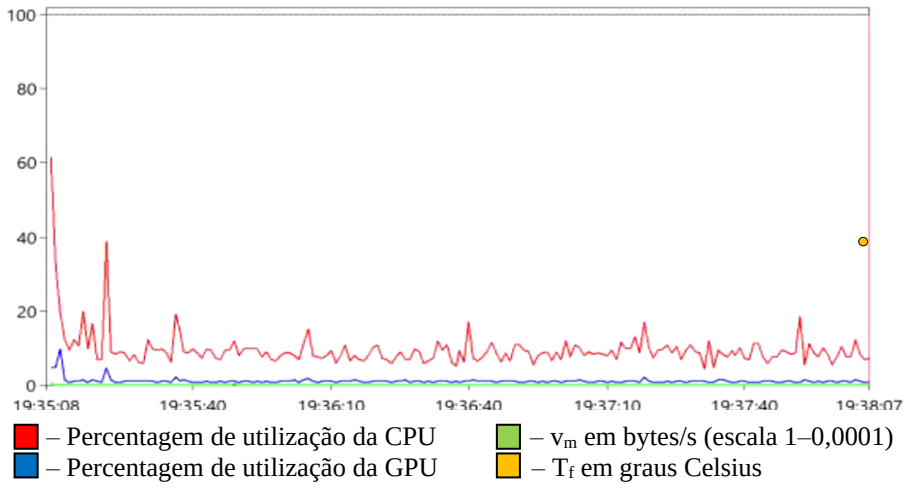

Figura n.º 11 – Resultados obtidos no teste de desempenho ao site n.º R2 (referência), a correr o Chrome no Android, durante 3 minutos.

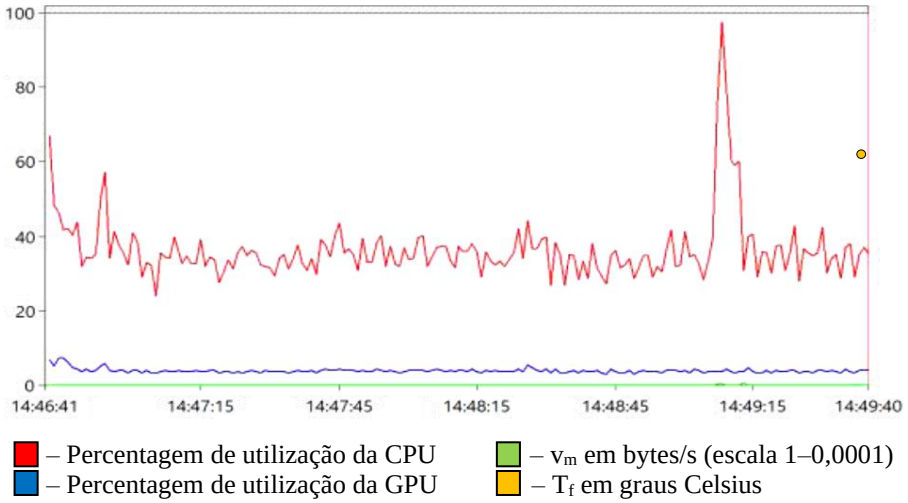

Figura n.º 12 – Resultados obtidos no teste de desempenho ao site n.º 18 (indiciado), a correr o Chrome no Android, durante 3 minutos.

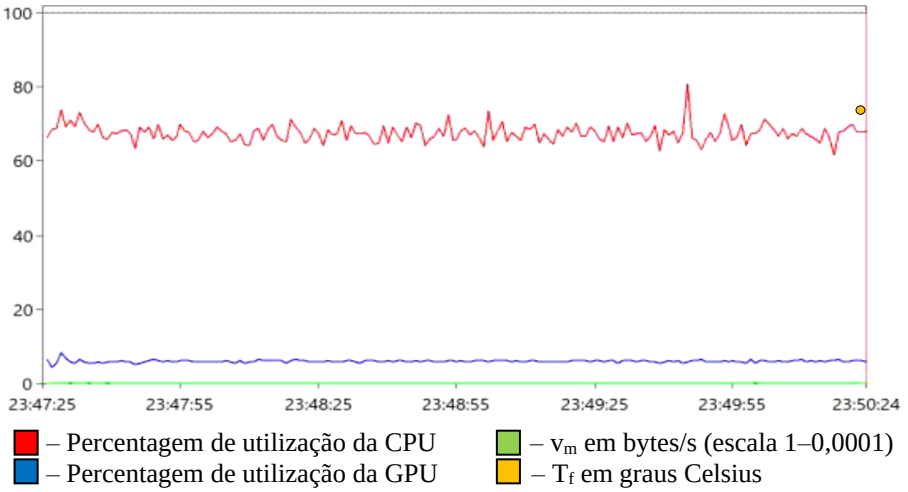

Figura n.º 13 – Resultados obtidos no teste de desempenho ao site n.º 84 (comprovado), a correr o Chrome no Android, durante 3 minutos.

Do total dos 400 testes realizados aos sites da amostra: 55 testes estavam dentro dos parâmetros definidos, levando a que 40 sites reunissem as condições para se considerarem, potencialmente, a minerar; 64 testes permitiram afirmar que 18 sites possuem efetivamente atividade de desempenho anormal, considerando-se que estão a minerar; e os restantes 331 testes indicaram que 42 sites se encontram, aparentemente, livres de *cryptojacking*.

Atendendo às categorias definidas, apresenta-se o gráfico da Figura n.º 14.

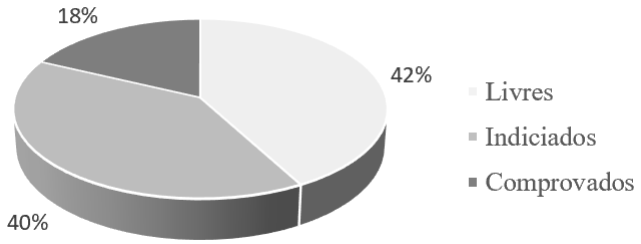

Figura n.º 14 – Resultados percentuais gerais para a presença de *cryptojacking* nos sites da amostra.

Constata-se que, no total, em 58% dos sites da amostra, há dados que sustentam a utilização de recursos para mineração, ficando também explícito que, na relação entre a quantidade de sites com indícios de *malware* e a de sites comprovadamente positivos, há maior preponderância para os primeiros, o que é compreensível, dado os critérios para enquadrar o site na categoria de "indiciado", serem menos exigentes.

Para melhor se verificar as diferenças entre os resultados obtidos, quando se dividem os sites pelas categorias anteriormente mencionadas, dispõe-se nas Figuras n.ºs 15, 16, 17 e 18, os gráficos tipo boxplot, comparativos de vários dados pertinentes ao estudo, os quais incluem:

- O valor mínimo e o valor máximo, sinalizados pelos extremos da linha vertical;
- Os valores atípicos, designados por *outliers*, e que, pela sua discrepância dos restantes valores, se encontram fora dos limites da dispersão, representados por um pequeno círculo;
- Uma caixa com os limites principais de dispersão, reunindo os valores entre o primeiro e o terceiro quartil, que representam o intervalo de maior concentração de registos;
- A média, assinalada com a linha horizontal no interior da caixa de limites de dispersão, e a mediana, representada por um "x".

Concretamente, é possível observar no gráfico da Figura n.º 15, que as percentagens médias de utilização da CPU nos sites de referência são as que possuem a dispersão mais reduzida, concentrando os resultados até aos 10%, apesar de existirem dois *outliers*. Nos sites indiciados como positivos, a dispersão é mais abrangente, contendo resultados entre os 5 e os 60%. Ainda assim, a maior parte dos registos encontra-se no espectro entre os 12% e os 34%.

No que diz respeito aos sites da categoria "comprovados", verifica-se uma maior dispersão de registos, mas a caixa de dispersão concentra-se entre os 23% e os 52%, significando que, em comparação, o valor correspondente ao primeiro quartil é muito semelhante à média da categoria "indiciados".

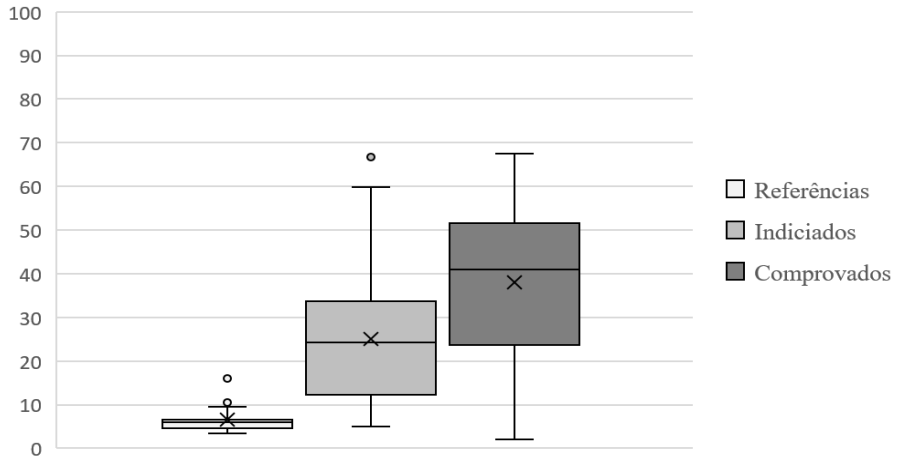

Figura n.º 15 – Boxplot comparativa dos valores de $\%CPU_m$, por categoria.

Quanto às temperaturas registadas no final de cada teste, pode constatar-se pelo gráfico da Figura n.º 16 que, novamente, os resultados dos testes de referência têm reduzida dispersão e concentram-se em torno dos 40ºC. Por sua vez, a temperatura final registada nos sites da categoria "indiciados", está disseminada entre os 39ºC e os 73ºC, com maior aglomeração entre os 50ºC e os 60ºC. Já na categoria "comprovados", o valor médio de 65ºC e os valores tendencialmente superiores, destacam-se das outras categorias.

Em suma, há diferenças significativas entre os sites de referência e os restantes.

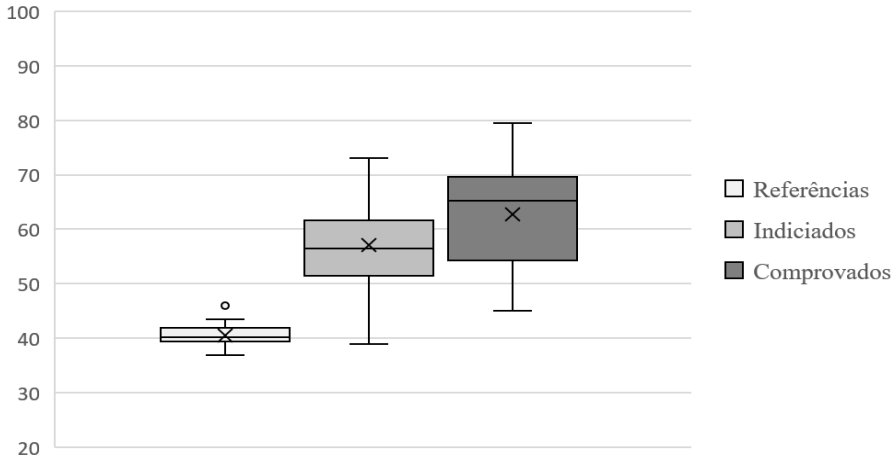

Figura n.º 16 – Boxplot comparativa dos valores de Tf_c, por categoria.

Em oposição aos dois gráficos anteriores, os que constam das figuras que se seguem, relativos, respetivamente, aos resultados de percentagem de utilização média da GPU e à velocidade média de transferência de dados, não atestam reveladoras diferenças entre as várias categorias de sites. É visível, em ambos os casos, uma fraca dispersão de valores, generalizada e similar entre as várias categorias de sites, acompanhada também por vários casos atípicos. Estes dados, poderão indicar que, as duas variáveis em consideração, não constituem bons indicadores da presença de *cryptojacking*, por se terem obtido valores bastante similares entre os sites de referência, que estão livres de *malware*, e as duas categorias de sites positivos da amostra, que se consideram infetados.

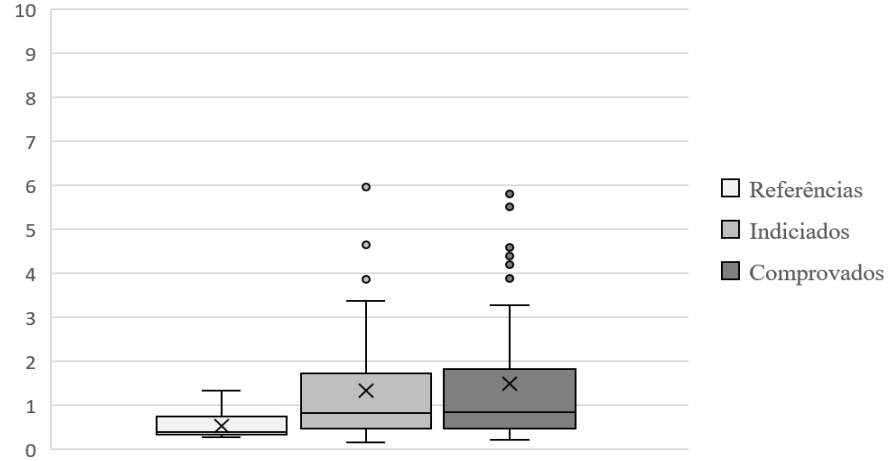

Figura n.º 17 – Boxplot comparativa dos valores de $\%GPU_m$, por categoria.

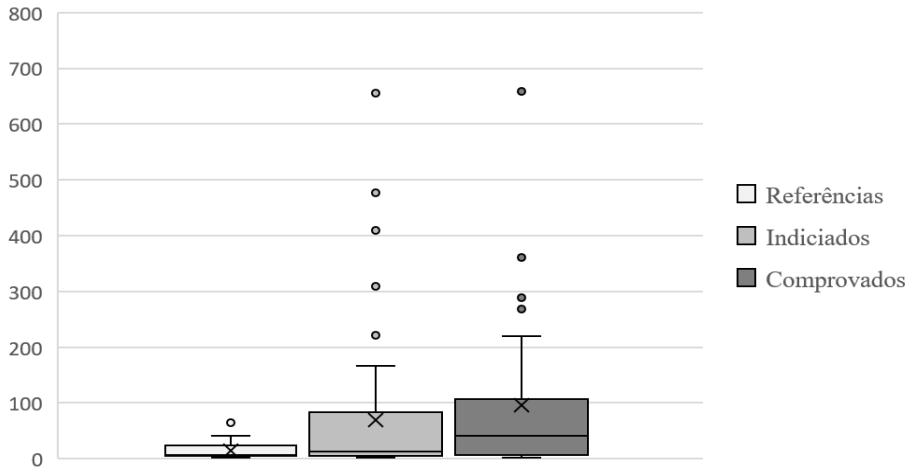

Figura n.º 18 – Boxplot comparativa dos valores de v_m, por categoria.

Para complementar as comparações gráficas efetuadas, calculou-se o desvio padrão para aferir se os valores registados tendem, ou não, a estar próximos dos valores médios. Deste modo, a Tabela n.º 5 contém os valores do desvio padrão amostral (*s*) para cada variável, em alusão aos sites de referência, aos indiciados positivos e aos comprovados positivos, descobrindo-se que, nos registos referentes à GPU, existe elevada consistência nos valores, dado não se afastarem consideravelmente da média. No caso da temperatura final, o desvio é muito reduzido para os sites de referência e aproxima-se dos 8ºC para os sites positivos.

Por outro lado, no que diz respeito aos registos da velocidade média de transferência, nas categorias de indiciados e comprovados, denota-se que existiram valores bastante discrepantes e que influenciaram o valor da média, conforme se pode observar na Tabela n.º 10 do Apêndice B, que integra, em detalhe, todos os resultados dos testes positivos.

Tabela n.º 5 – Resultados para o desvio padrão aplicado às várias categorias de sites.

Categoria do site	*s* %$CPU_{máx}$	*s* %$CPU_{mín}$	*s* %CPU_m	*s* %$GPU_{máx}$	*s* %$GPU_{mín}$	*s* %GPU_m	*s*Tf_c	*s*v_m
Referência	20,15	1,09	2,90	2,39	0,14	0,30	2,13	16,13
Indiciados	19,33	16,54	15,66	4,69	1,14	1,33	7,92	129,25
Comprovados	15,80	19,37	16,36	4,83	1,04	1,48	8,82	173,90

Para esclarecimento final sobre a relevância destes dados recolhidos, calculou-se também, com base em todos os testes positivos, o coeficiente de correlação de Pearson entre a percentagem média de utilização da CPU e a temperatura, obtendo-se um resultado de p=0,69, que indica uma relação positiva moderada, ou seja, quando o registo da CPU aumenta, a temperatura tende a subir. Para a correlação entre a percentagem média de utilização da CPU e a velocidade média de transferência obteve-se p=-0,06, significando que não há qualquer relação plausível entre estas variáveis, no contexto dos testes efetuados.

Pelo exposto, considera-se que é pertinente observar a temperatura final registada e que não é fiável utilizar os valores da velocidade de transferência média para aferir a presença do *malware*, apesar das diferenças notórias no gráfico comparativo de médias.

4.3. Análise de resultados

De seguida, através do gráfico da Figura n.º 19, verifiquem-se os resultados estatísticos referentes ao sucesso das plataformas online utilizadas inicialmente para identificar sites que estivessem a correr *malwares* de mineração. Para isso, apurou-se, de entre os 58 sites que apresentaram resultados positivos, quais os que tinham sido previamente referenciados, constatando-se que, com exceção da plataforma Publicwww, da qual se extraiu a listagem para amostra, o Notmining foi mais eficaz, detetando 31 sites, em contraste com os 23 sites reconhecidos pelo Wappalyzer.

Quanto aos que possuíam aviso para a mineração aquando da abertura do site, verifica-se que apenas sete, dos oito sites com aviso, foram considerados como estando a minerar. Para informação mais detalhada acerca das plataformas que identificaram cada site, em particular, que se categorizou como positivo, consulte-se a Tabela n.º 11 do Apêndice B.

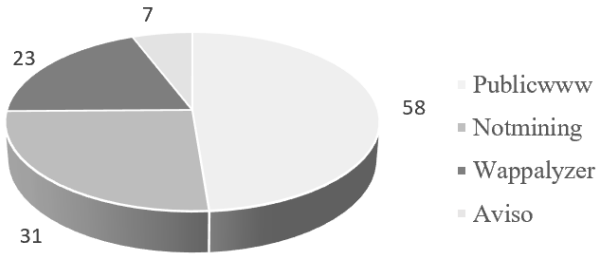

Figura n.º 19 – Quantidade de sites positivos identificados por cada plataforma, ou que apresentou aviso para a mineração no próprio site.

Pela análise ao gráfico da Figura n.º 20, retira-se que, dos 58 sites determinados como positivos para *cryptojacking*, 67% foram identificados por duas ou mais plataformas, havendo apenas 19 sites a ser identificados exclusivamente pela plataforma inicial – o Publicwww. Pelo conjunto das três plataformas, foram identificados 17 sites positivos, valor que se considera reduzido, por não contemplar, sequer, um terço dos casos.

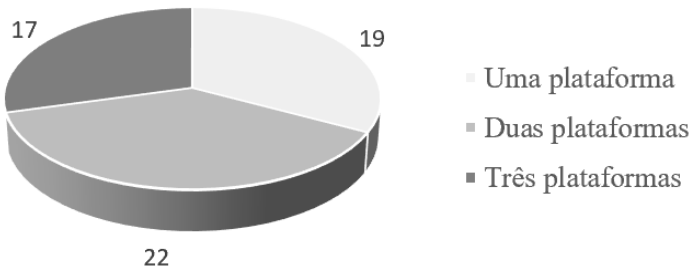

Figura n.º 20 – Quantidade de sites positivos e respetivo número de plataformas, em que, inicialmente, foram identificados.

Nas figuras seguintes, podem ser visualizadas informações adicionais relativas ao resultado dos 400 testes concretizados à amostra. Desses testes, relembra-se que 200 correram em MV com Windows, 100 em MV com Android e 100 em MV com Linux. No que aos *browsers* diz respeito, 200 testes tiveram lugar com utilização do Chrome e os restantes 200 com uso do Firefox.

Tal como consignado na parte inicial do presente subcapítulo, delinearam-se critérios para enquadramento dos sites com resultados positivos em duas categorias (indiciados e comprovados), com base no número de testes que atingiram determinados valores mínimos. As figuras seguintes incorporam a divisão, por SO e *browsers*, dos 119 testes com resultados positivos – ou seja, que originaram uma percentagem média de utilização da CPU igual, ou superior, a 20% e/ou geraram uma temperatura final da CPU igual, ou superior, a 50ºC.

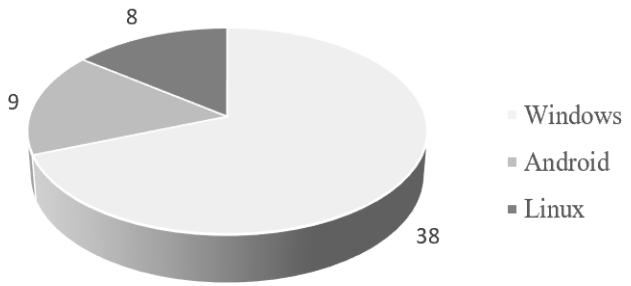

Figura n.º 21 – Número de testes positivos da categoria "indiciado", por OS.

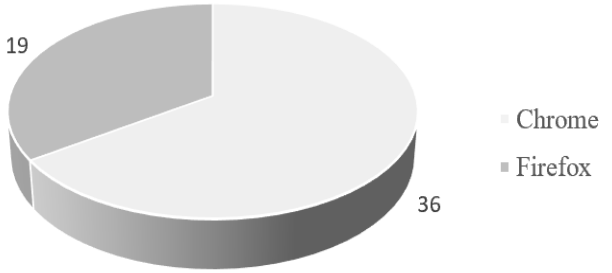

Figura n.º 22 – Número de testes positivos da categoria "indiciado", por *browser*.

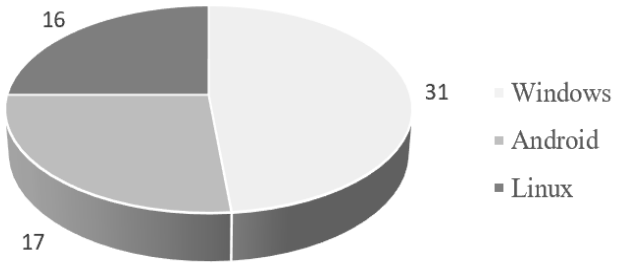

Figura n.º 23 – Número de testes positivos da categoria "comprovado", por OS.

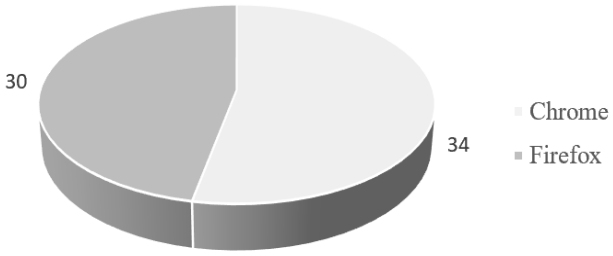

Figura n.º 24 – Número de testes positivos da categoria "comprovado", por *browser*.

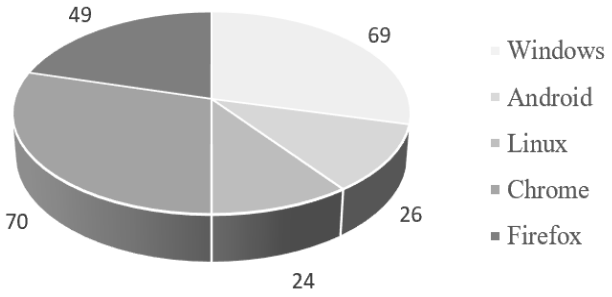

Figura n.º 25 – Número de testes que obtiveram resultados positivos, dentro de cada OS e *browser*.

Continuamente, passa-se à apresentação de duas tabelas com informação estatística mais pormenorizada. A Tabela n.º 6, que integra o conjunto de resultados positivos, obtidos para cada OS e *browser* utilizado, denota que para a categoria "indiciados", a quantidade de resultados utilizando o Chrome no Windows, foi bastante superior à do Chrome no Android. No que diz respeito à categoria "comprovados", o número de resultados foi semelhante para todos os OS e *browsers*. O total de positivos, é também similar para os testes em Android, Linux e Firefox no Windows, havendo um grande destaque para o primeiro conjunto de testes executado, em Chrome no Windows, que resulta em 44% dos sites positivos para mineração, face aos cerca de 25% dos restantes conjuntos de testes.

Tabela n.º 6 – Resultados para a presença de *cryptojacking* nos sites da amostra, por *browser* e SO.

Browser	SO	Amostra	Indiciados	Comprovados	Total positivos	Percentagem positivos
Chrome	W	100	**27**	**17**	**44**	**44%**
	A	100	9	**17**	26	26%
Firefox	W	100	11	14	25	25%
	L	100	8	16	24	24%

Legenda: "Negrito" – Valor mais elevado da categoria; **W –** Windows; **A –** Android; **L –** Linux.

Por sua vez, a informação constante na Tabela n.º 7, dispõe os resultados detalhados com base no *script* utilizado, extraindo-se que o JSEcoin é o que contém mais sites da amostra para a categoria "indiciados" e em quantitativo total de positivos, enquanto que o CoinImp possui o maior número de sites para a categoria "comprovados".

Tabela n.º 7 – Resultados para a presença de *cryptojacking* nos sites da amostra, por tipo de *script*.

Designação	Amostra	Indiciados	Comprovados	Total positivos	Percentagem positivos
CoinHive	20	9	1	11	55%
Crypto-Loot	20	8	1	9	45%
CoinImp	20	4	**8**	12	60%
deepMiner	20	6	5	11	55%
JSEcoin	20	**13**	3	**16**	**80%**

Legenda: "Negrito" – Valor mais elevado da categoria.

Em termos percentuais, o JSEcoin obteve uma taxa de 80% de sites positivos para *cryptojacking*, de entre os testados, seguindo-se o CoinImp com 60%. Apenas o Crypto-Loot não superou a metade dos sites testados como estando infetados, ficando-se pelos 45% de positivos. O CoinImp surge como exceção nesta vertente, por ter somente quatro sites indiciados por *cryptojacking*, o valor mínimo de entre todos os *scripts*.

Como parte da análise de resultados, cabe ainda aludir a alguns resultados observados durante a execução dos testes e que, por se considerarem detentores de particularidades ou diferentes do espectável, se consideram dignos de menção e eventual estudo futuro.

No decorrer dos testes, observaram-se alguns detalhes de interesse e resultados particulares, dos quais se destaca que:

- Os sites visualmente mais apelativos ou com mais conteúdos, sobretudo de multimédia (vídeo e som), demonstram ter um período inicial de carregamento mais elevado, o que se transcreve numa utilização incomum de recursos do sistema (atividade da CPU e da GPU), que poderia ser confundida com mineração. Nos testes efetuados, o período de três minutos de duração permitiu eliminar, à partida, esses falsos positivos, pois após o carregamento do site estar completo, verificou-se uma descida drástica no consumo de recursos, que assim se manteve até ao fim da experiência. Para um exemplo gráfico desta ocorrência, examine-se a Figura n.º 26;

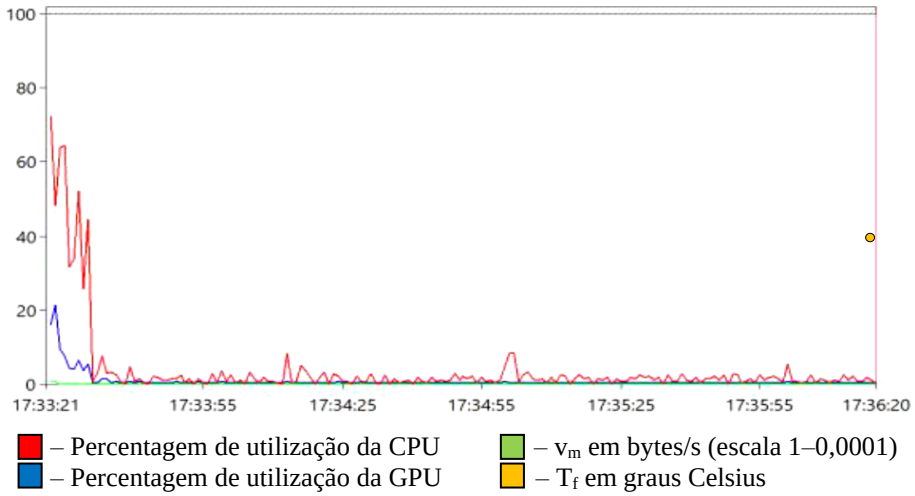

Figura n.º 26 – Resultados obtidos no teste de desempenho ao site n.º 38, a correr o Chrome no Android, durante 3 minutos.

- Em diversos casos, registou-se uma percentagem de utilização da CPU inicial bastante elevada, com duração de alguns segundos, após os quais reduzia drasticamente e se mantinha mínima. Sem prejuízo do disposto no ponto anterior, estes casos, normalmente mais extremos na utilização da CPU e que não afetam a utilização da GPU, poderão ser também um indicador de *malware*, uma vez que há *scripts* de *cryptojacking* que testam primeiro o poder de processamento e a capacidade de mineração da máquina alvo, e só se executam se os valores estiverem dentro dos parâmetros de rentabilidade definidos pelo seu programador. Para um gráfico exemplo desta ocorrência, que pode constituir um falso negativo, veja-se a Figura n.º 27;

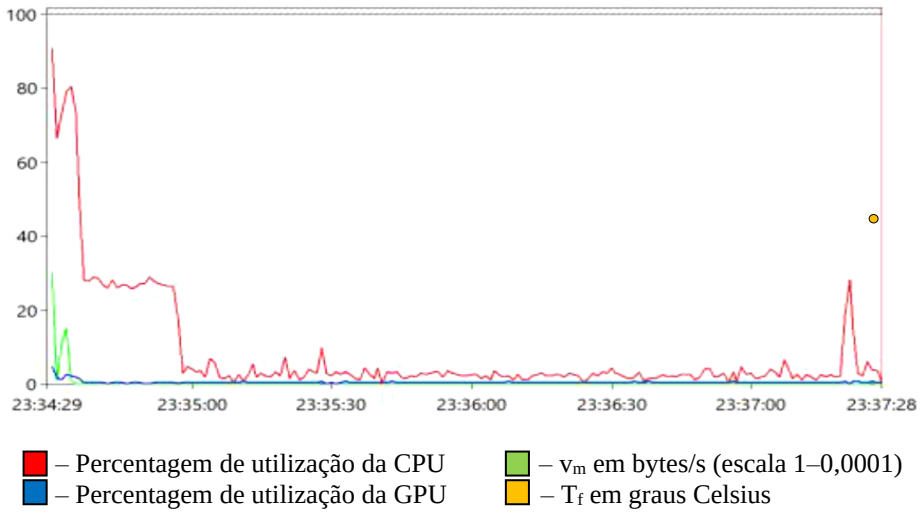

Figura n.º 27 – Resultados obtidos no teste de desempenho ao site n.º 25, a correr o Chrome no Windows, durante 3 minutos.

- Alguns sites da amostra pertenciam a empresas, agências noticiosas (site n.º 14) ou até a departamentos estatais, como é o caso do site n.º 51 (`insai.gob.ve`), que corresponde ao "Instituto Nacional de Salud Agrícola Integral", do Governo da Venezuela. Neste caso concreto, não foi possível comprovar a mineração através dos testes, mas alerta-se o facto do site constar na listagem da amostra e ter sido identificado como tendo o *script* do CoinImp. Estes dados reiteram o aproveitamento de fragilidades conhecidas nos sistemas e nos sites, que permitem a um agente mal intencionado introduzir o *script* de mineração, sem que os detentores dos sites se apercebam, passando a lucrar com os acessos aos mesmos e dissimulando a sua atividade por estarem a utilizar sites que os utilizadores reconhecem como fidedignos;

- A Figura n.º 28, apresenta o gráfico obtido para um teste ao site n.º 30 e distingue-se pelo padrão de irregularidade da utilização percentual da CPU, no qual se registam repetidamente, a partir dos 30 segundos de teste, máximos na ordem dos 35%, seguidos de mínimos próximos dos 0%. Em teoria, isto poderia ocorrer quando um site tentar correr um *script* e, por algum motivo, não seja possível executá-lo naquele momento. Outra justificação poderia englobar uma tentativa de mineração que acabasse por não

acontecer, por haver deteção da MV ou da abertura do medidor de desempenho. É, de todo o modo, importante referir que, apesar da aparente baixa utilização média da CPU, registou-se a temperatura de 59ºC, no fim do teste ao Chrome a correr no Windows, e 52ºC, no do Firefox a correr no Windows, tendo por isso, sido enquadrado na categoria de "indiciado" como positivo. É um exemplo particular, em que se supõe que possa existir código embutido no *script* que condicione a correta medição do desempenho;

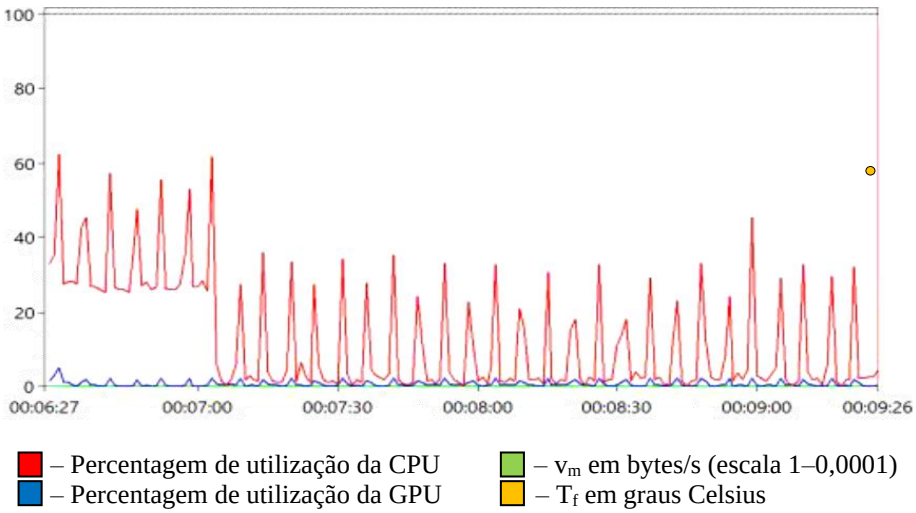

Figura n.º 28 – Resultados obtidos no teste de desempenho ao site n.º 30, a correr o Chrome no Windows, durante 3 minutos.

- Podem existir sites a correr atividade de mineração, mas com *scripts* mais avançados e que detetem se o *browser* se encontra a executar-se dentro de ambientes de análise. Caso encontrem definições oriundas de uma MV, de um ambiente de testes ou de um *browser* a correr dentro de uma *sandbox*, não ativam a sua atividade, o que não permitirá a análise dos seus efeitos. Acredita-se que, em alguns dos sites da amostra, isto terá ocorrido, com particular atenção aos sites que foram identificados pelas três plataformas como estando a correr *cryptojacking*, mas cujos testes não permitiram comprovar, como é o caso do site n.º 6;

- A Figura n.º 29 exemplifica outro caso particularmente anormal, talvez dos mais perspicazes na conceção e eficazes no funcionamento, no qual há um período inicial de carregamento do site com alguma inconstância na utilização de recursos, mas sem dados alarmantes, e ao fim de dois minutos, inicia-se uma atividade clara de mineração, aparentemente programada para consumir cerca de 50% do poder de processamento do sistema. É significativo que se tenham detetado estes resultados incomuns, pois manifestam a importância da duração estabelecida para os testes. Caso fosse ligeiramente mais curto, o teste poderia não ter detetado este método de funcionamento do *script*. É um sistema de funcionamento especialmente enganador para os utilizadores, pois para além de dificultar a sua deteção, por estar a utilizar apenas metade da capacidade de processamento, ainda dispõe de um período de ativação ou de

um ativador relacionado com os lucros mínimos pretendidos, fazendo com que se reduza a relação causa (abertura de um site) e efeito (sistema mais lento);

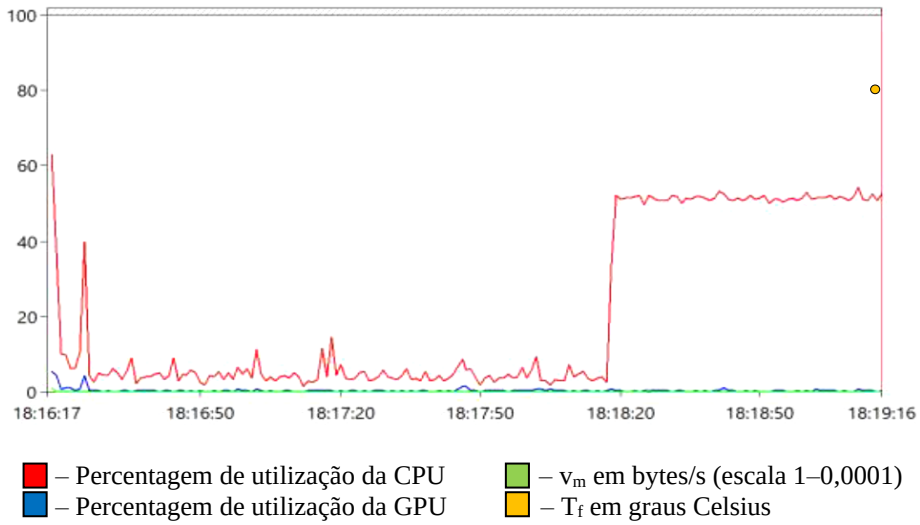

Figura n.º 29 – Resultados obtidos no teste de desempenho ao site n.º 57, a correr o Chrome no Android, durante 3 minutos.

- A par do que demonstra a Figura n.º 30, houve alguns sites que iniciaram a utilização da CPU durante um certo período, após o qual terminaram essa atividade e passaram a valores mais reduzidos. Alguns, mantiveram essa redução durante o restante período da experiência, aparentando deixar de minerar. Outros, como este caso em concreto, voltaram a aumentar os registos, passado algum tempo. Considera-se que estes casos possam, igualmente, estar relacionados com as definições do atacante para a rentabilidade da mineração.

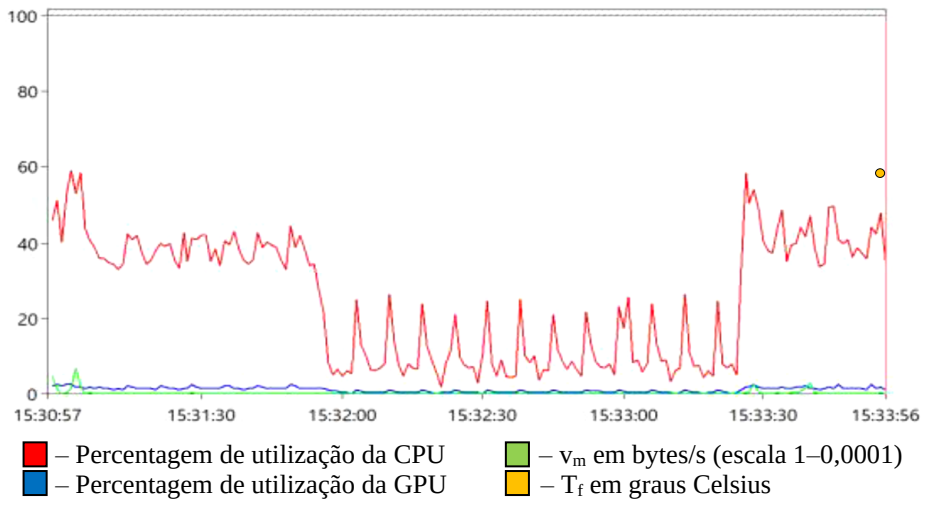

Figura n.º 30 – Resultados obtidos no teste de desempenho ao site n.º 22, a correr o Firefox no Linux, durante 3 minutos.

Capítulo 5

Conclusão

O último capítulo do presente trabalho é o culminar de todas as restantes partes constituintes, procurando-se dar resposta às questões derivadas e finalmente à questão principal de partida da investigação, bem como proceder-se à confirmação ou refutação das hipóteses concebidas no começo, na parte introdutória do trabalho.

5.1. Questões derivadas

Questão Derivada n.º 1: **Quais os fatores associados à evolução e disseminação do *cryptojacking*?**

Hipótese n.º 1.1: **O valor de mercado das criptomoedas.**

A hipótese confirma-se parcialmente, na medida em que ficou comprovado pela revisão de literatura que os hiatos temporais em que houve maior subida do valor de criptomoedas (Figuras n.º 1, 2 e 3), aparentam corresponder, às alturas em que houve maior quantidade geral de *malwares* ligados à mineração (Figura n.º 4).

Também na parte prática, conseguiu-se confirmar parcialmente esta afirmação, dado que Eskandari *et al.* (2017) e Mursch (2018) obtiveram respetivamente, no final de 2017 e no início de 2018, uma listagem bastante superior de sites a correr o CoinHive, principal ator utilizado para mineração à data (p. 19 e 27), quando em comparação com os resultados de replicação da sua experiência (Tabela n.º 3).

Hipótese n.º 1.2: **O grau de dificuldade de mineração.**

A hipótese confirma-se parcialmente, uma vez que, pela revisão bibliográfica, constata-se que a dificuldade de mineração aumenta (p. 11), à medida que são descobertos novos blocos e adicionados à *blockchain*, passando a exigir-se, cada vez mais poder de processamento para manter a rentabilidade.

De todo o modo, no presente estudo, não se comprova diretamente que a disseminação de *cryptojacking* enfraqueça, com base no aumento do nível de complexidade, tratando-se esta conclusão apenas de análise teórico-lógica, no sentido em que o *cryptojacking* visa a obtenção de lucro para o atacante, e com o aumento da dificuldade em o gerar deste modo,

outras alternativas, como o *ransomware*, o *phishing* ou o *skimming* (fraude envolvendo cartões de pagamento), voltam a tomar parte.

Questão Derivada n.º 2: **Qual a significância dos vários tipos de *cryptojacking* para o desempenho do dispositivo afetado?**

Hipótese n.º 2.1: **Alguns *malwares* de *cryptojacking* atuam de diferente modo, consoante as particularidades do sistema/*browser* afetado.**

A hipótese confirma-se parcialmente, quer pela descrição dos métodos de funcionamento do *cryptojacking* (p. 16) e pelos conteúdos da Tabela n.º 2, na parte teórica, quer pela constatação de alguns resultados da parte prática, nomeadamente pelos conteúdos da Tabela n.º 6 e n.º 7, e pelas Figuras n.º 21 a 25.

Em suma, comprovou-se que, testando o mesmo site, segundo os mesmos parâmetros, em quatro ambientes diferentes, alterando-se o SO e o *browser*, os resultados foram distintos, concluindo-se que há alterações na forma de atuação do *malware* de *cryptojacking*. Essas disparidades poderão dar-se, p. ex., pelo facto do *script* estar otimizado para correr em determinados contextos, ou para ser bloqueado noutros (p. 42 e 43).

Hipótese n.º 2.2: **Quanto menor o efeito no desempenho do dispositivo da vítima, mais difícil será a deteção do ataque.**

A hipótese confirma-se totalmente, uma vez que, em contexto teórico, o *malware* pode ser descoberto por análise de padrões ou por observação de efeitos (p. 8). Isto significa que, quanto menos percetíveis forem os sinais indicadores de que algo errado afetou um sistema, mais complexa será a sua deteção, segundo o aforismo de que "não se procura o que não se sabe que existe".

Inclusivamente, comprovou-se que há serviços online que permitem a qualquer utilizador comum, introduzir *scripts* de mineração num site que administre, selecionando opções que reduzam a sua evidência (p. 18) – limitando o poder de processamento, introduzindo um intervalo de atraso para iniciação da mineração, bloqueando os seus efeitos a programas de análise de desempenho, ou simplesmente não correndo quando detetarem que o acesso se faz a partir de uma MV (p. 41 a 44).

Questão Derivada n.º 3: **É possível detetar um ataque de *cryptojacking*, pela análise de desempenho do sistema afetado?**

Hipótese n.º 3.1: **Para a mineração ser eficaz e lucrativa, a forma como o desempenho da CPU ou da GPU é afetado por essa atividade, apresenta padrões reconhecíveis.**

A hipótese confirma-se parcialmente, quer pelo facto de, atualmente, o valor das criptomoedas estar a atravessar uma fase menos rentável (Figura n.º 1, 2 e 3, e Tabela n.º 3), quer porque, cada vez mais, será necessário maior poder de processamento para manter a

rentabilidade. Isto significa que, embora em teoria, o agente mal-intencionado possa restringir a utilização de recursos para o valor que entender (p. 18), para que a atividade seja "eficaz e lucrativa", presume-se, com base nos dados recolhidos, que a mesma origine indícios que possam ser analisados.

Observando-se os resultados para os sites de referência (Tabela n.º 4), pode considerar-se que não estarão a minerar (pelo menos, de forma lucrativa), as máquinas que apresentem valores de utilização médios de CPU inferiores a 20%, tal como considerado para a categorização dos resultados positivos no presente estudo (p. 33).

É, de todo o modo, relevante referir, que no âmbito da experiência concretizada, não houve registos de valores da GPU, nos testes à amostra, que se destacassem, quando em comparação com os valores obtidos para os sites de referência (Figura n.º 17). Por este facto, considera-se que, somente a afetação do desempenho da CPU poderá ser um bom indicador, no que concerne à presença de *cryptojacking browser-based*.

Hipótese n.º 3.2: **Existem outros fatores que podem provocar os mesmos sintomas nos sistemas.**

A hipótese confirma-se parcialmente, uma vez que, os resultados considerados positivos, obtidos através dos testes práticos, indicam a existência de atividade de processamento com valores anormais (Figura n.º 11, 12 e 13) em diversos casos de *cryptojacking*, os quais poderiam confundir, um utilizador comum, quanto ao tipo de atividade que estaria a originar sintomas caraterísticos deste *malwares*, como o incremento do consumo de recursos do sistema, o aumento da temperatura, ou a perceção de um sistema mais lento a responder a novas solicitações.

Pelo conjunto de testes corridos, pode observar-se que, mesmo para os resultados que se consideraram positivos, obtiveram-se alguns gráficos de desempenho diferentes entre si (Figura n.º 12, 13, 28, 29, 30). Não se testou a máquina a correr jogos ou vídeo de alta resolução, mas de acordo com a teoria, essas atividades têm potencial para dar origem ao mesmo tipo de sintomas.

Questão Derivada n.º 4: **Para além da análise ao desempenho da CPU ou da GPU, existem outras variáveis pertinentes para a deteção do *cryptojacking*?**

Hipótese n.º 4.1: **É relevante atentar também à temperatura atingida pelo sistema.**

A hipótese confirma-se totalmente, quer pela menção desse efeito na revisão bibliográfica (p. 17), quer pela parte prática, tendo-se também em consideração que houve sites em que não se conseguiu detetar corretamente o aumento no desempenho, mas registou-se uma temperatura final que não correspondia aos restantes dados recolhidos (Tabela n.º 10).

Estes dados levaram a que a variável – temperatura final da CPU – fosse observada aquando da classificação de testes e sites na categoria de "resultados positivos" (p. 33).

Mais adiante, confirmou-se que a temperatura final da CPU era um indicador de consistência intermédia, obtendo-se uma relação positiva moderada, de p=0,69, para o

coeficiente de correlação de Pearson, entre a percentagem média de utilização da CPU e a temperatura final (p. 37).

Hipótese n.º 4.2: **É relevante considerar a velocidade de transferência de dados entre o sistema e a internet.**

A hipótese não se confirma, pela fraca diferença de valores obtidos para as várias categorias, pela existência de vários *outliers* (Figura n.º 18) e, sobretudo, os valores do desvio padrão da variável v_m foram bastante elevados para as categorias de sites positivos (Tabela n.º 5), comprovando-se que, no âmbito dos testes realizados, não há qualquer relação entre desempenhos elevados e velocidade média de transferência de dados.

5.2. Questão de partida

Quais as principais caraterísticas do *cryptojacking*, a sua relevância atual e os efeitos que provocam no sistema afetado?

Em resposta à questão de partida, na qual se centra o trabalho, cumpre agora tecer as considerações finais. Relativamente às suas características, encontrou-se na revisão de literatura algumas formas de categorização de *malwares* de mineração: baseado na máquina / baseado na *web*, conforme atue localmente no sistema, através de *software* instalado, ou pelo acesso a determinados sites através do *browser*; persistente / não persistente – consoante a mineração indesejada se mantenha independentemente do site com o *script* estar aberto, ou cesse a sua atividade quando o utilizador muda de separador ou feche o site;

A importância do estudo do *cryptojacking* advém da sua descoberta ser relativamente recente, das implicações que acarreta para os utilizadores de sistemas afetados e da falta de fontes bibliográficas de cariz científico para abordar o tema, com exceção de alguns relatórios de empresas ou autores da área da cibersegurança. Ao mesmo tempo que os valores das criptomoedas ascenderam, a disseminação destes *malwares* propagou-se, para máximos no primeiro semestre de 2018, encontrando-se desde então em declínio, conforme comprova o relatório de ameaças da Symantec (2019, p. 15).

Atualmente, a elevada dificuldade de lucrar através de mineração, tanto pelo reduzido valor das criptomoedas, como pelo aumento da complexidade na descoberta de novos blocos, tem originado o término de serviços de mineração legítimos e dissuadido novos ataques *cryptojacking*, sendo 2019 caraterizado pelo aumento de outros ataques, e pela elevada incidência de *formjacking* (roubo de informação comercial ou bancária).

Quanto aos efeitos, conseguiu-se provar, através da parte prática, que o desempenho é influenciado de diversos modos, consoante os parâmetros do *script* do *malware*, afetando maioritariamente o desempenho da CPU. Nos testes executados, para *cryptojacking* baseado no *browser*, não se verifica influência no desempenho da GPU.

Por fim, o presente estudo conclui que a temperatura atingida pela CPU deve ser igualmente considerada para a deteção de *cryptojacking*, ao contrário da velocidade total de transferência de dados, registada durante o período de mineração.

5.3. Investigações futuras e encerramento

Aconselha-se que, para investigações futuras acerca da mesma matéria, se efetuem testes repetitivos e, eventualmente, com maior duração, à amostra de sites, para obtenção de registos com maior significância e que possam conter fenómenos que não foram passiveis de observar como os parâmetros da experiência atual. Neste âmbito, poderá p. ex., analisar-se o que terá efetivamente ocorrido na MV, no SO, no *browser*, ou no próprio *script* de mineração, para que, dos 100 sites da amostra, 42 não tivessem apresentado efeitos dessa atividade no desempenho.

Do mesmo modo, seria interessante efetuar os testes em computadores dedicados ou em laboratório, com o intuito de poder comparar os efeitos, face aos resultados obtidos em MV, bem como testar a eficácia de extensões, para *browsers*, que aleguem ter mecanismos para proteger o utilizador de *cryptojacking*, ou que funcionem com uma *blacklist* de sites identificados com os *scripts*.

Propõe-se a elaboração de uma investigação, com vista a apurar a existência de outras variáveis não consideradas no presente estudo e que possam prever, influenciar ou detetar a presença de mineração ilícita em sistemas, tais como, observando os processos em execução, examinando o código dos *scripts* a correr nos sites, ou medindo os valores de voltagem.

Encerra-se com a perspetiva de ter colaborado no enquadramento e análise do objeto em apreço, tendo presente a dificuldade acrescida da escassa bibliografia de referência para a temática, o que obrigou à reunião de dados de diversas fontes e em larga escala, efetuando-se o seu cruzamento para obtenção de informação fiável.

Deseja-se que este breve contributo, alusivo à identificação e análise dos efeitos de *cryptojacking* no desempenho, possa servir de apoio a futuros trabalhos, em prol do desenvolvimento das novas tecnologias e da melhoria da segurança da informação.

Referências bibliográficas

1. 360 Total Security: CryptoMiner, WinstarNssmMiner, Has Made a Fortune By Brutally Hijacking Computers (2018), https://blog.360totalsecurity.com/en/cryptominer-winstarnssmminer-made-fortune-brutally-hijacking-computer, acedido em 2019/01/27.
2. AItken, R.: Does Venezuela's Oil-Backed 'Petro' Have The Power To Showcase National Cryptocurrencies? (2018), https://www.forbes.com/sites/rogeraitken/2018/05/31/does-venezuelas-oil-backed-petro-have-the-power-to-showcase-national-cryptocurrencies/#a86b83c7b436, acedido em 2019/01/22.
3. AMR: Kaspersky Security Bulletin 2018 – Statistics (2018), https://securelist.com/kaspersky-security-bulletin-2018-statistics/89145, acedido em 2018/12/28.
4. Arnold, A.: 30% Of Millennials Would Rather Invest In Cryptocurrency (2018), https://www.forbes.com/sites/andrewarnold/2018/01/07/30-of-millennials-invest-in-cryptocurrency-here-are-3-tips-to-help-you-do-it-smarter, acedido em 2018/12/07.
5. Aslam, N.: Banks Banning Cryptocurrency Purchase On Credit Cards, Why? (2018), https://www.forbes.com/sites/naeemaslam/2018/02/05/banks-banning-cryptocurrency-purchase-on-credit-cards-why, acedido em 2018/12/19.
6. BBC: Cyber-attack – Europol says it was unprecedented in scale (2017), https://www.bbc.com/news/world-europe-39907965, acedido em 2019/01/02.
7. Bissaliyev, M., Nyussupov, A. e Mussiraliyeva, S.: Enterprise Security Assessment Framework for Cryptocurrency Mining Based on Monero. Journal of Mathematics, Mechanics and Computer Science, 98, 67-76 (2018).
8. CAPEC: About CAPEC – Objective (2018), https://capec.mitre.org/about/index.html, acedido em 2018/12/26.
9. CAPEC: CAPEC-186 – Malicious Software Update (2018a), https://capec.mitre.org/data/definitions/186.html, acedido em 2018/12/26.
10. CAPEC: CAPEC-88 – OS Command Injection (2018b), https://capec.mitre.org/data/definitions/88.html, acedido em 2018/12/26.
11. CAPEC: CAPEC-443 – Malicious Logic Inserted Into Product Software by Authorized Developer (2018c), https://capec.mitre.org/data/definitions/443.html, acedido em 2018/12/26.
12. CAPEC: CAPEC-549 – Local Execution of Code, https://capec.mitre.org/data/definitions/549.html, acedido em 2018/12/26.
13. Check Point: Crypto Miners – The Silent CPU Killer of 2017 (2018), https://blog.checkpoint.com/2017/10/23/crypto-miners-the-silent-cpu-killer-of-2017, acedido em 2019/01/28.
14. Cisco: Cisco 2018 Annual Cybersecurity Report. Cisco Systems (2018).
15. Cisco: Cybersecurity Special Report – Small and Mighty – How Small and Midmarket Businesses Can Fortify Their Defenses Against Today's Threats. Cisco Systems (2018a).

16. CoinImp: Documentation of Monero JavaScript Mining (2019), https://www.coinimp.com/documentation, acedido em 2019/03/27.
17. Cyber Threat Alliance: The Illicit Cryptocurrency Mining Threat (2018), https://www.cyberthreatalliance.org/wp-content/uploads/2018/09/CTA-Illicit-CryptoMining-Whitepaper.pdf, acedido em 2019/09/27.
18. Egele, M., Scholte, T., Kirda, E., e Kruegel, C.: A Survey on Automated Dynamic Malware-Analysis Techniques and Tools. ACM Computing Surveys, Vol. 44, No. 2, Article 6, 2-42 (2012).
19. Eilam, E.: Reversing: Secrets of Reverse Engineering. John Wiley & Sons, Inc. New Jersey (2011).
20. European Union Agency for Network and Information Security (ENISA): Cryptojacking – Cryptomining in the browser (2017), https://www.enisa.europa.eu/publications/info-notes/cryptojacking-cryptomining-in-the-browser, acedido em 2019/01/18.
21. Eskandari, S., Leoutsarakos, A., Mursch, T., Clark, J.: A First Look at Browser-Based Cryptojacking. IEEE Security & Privacy on the Blockchain (2018).
22. Evangelho, J.: Nvidia CEO – "We're Not Anywhere Near" Meeting GPU Demand (2018), https://www.forbes.com/sites/jasonevangelho/2018/03/27/nvidia-ceo-were-not-anywhere-near-meeting-gpu-demand, acedido em 2018/11/27.
23. Galal, H., Mahdy, Y. e Atiea, M.: Behavior-based features model for malware detection. Journal of Computer Virology an Hacking Techniques, ISSN 2274-2042, Vol. 2, Issue-8, 54-56 (2015).
24. Grimes, R.: 8 types of malware and how to recognize them (2018), https://www.csoonline.com/article/2615925/security/security-your-quick-guide-to-malware-types.html, acedido em 2018/11/02.
25. Ioannou, N.: Internet Security Fundamentals – A Modern Day Digital Survival Guide, Boolean Logical Ltd., United Kingdom (2018).
26. Ismail, N.: Artificial Intelligence technologies could boost capabilities of hackers (2018), https://www.information-age.com/ai-technologies-boost-capabilities-hackers-123470960, acedido em 2019/01/02.
27. Jones, S.: Timeline – How the WannaCry cyberattack spread (2017), https://www.ft.com/content/82b01aca-38b7-11e7-821a-6027b8a20f23, acedido em 2019/01/04.
28. Kaspersky: 10 Signs of a Malware Infection (2013), https://www.kaspersky.com/blog/signs-of-malware-infection/2505, acedido em 2019/01/18.
29. Kharpal, A.: Hackers who infected 200,000 machines have only made $50,000 worth of bitcoin, https://www.cnbc.com/2017/05/15/wannacry-ransomware-hackers-have-only-made-50000-worth-of-bitcoin.html, acedido em 2019/01/13.
30. Khade, K. e Lin, X.: WebCobra Malware Uses Victims' Computers to Mine Cryptocurrency (2018), https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/webcobra-malware-uses-victims-computers-to-mine-cryptocurrency, acedido em 2019/01/04.
31. Kleinman, L.: A New Age Of Malware – Cryptocurrency Mining (2018), https://www.forbes.com/sites/forbestechcouncil/2018/06/07/a-new-age-of-malware-cryptocurrency-mining, acedido em 2018/12/07.
32. Křoustek, J.: Meet Adylkuzz – Cryptocurrency-mining malware spreading using the same exploit as WannaCry (2017), https://blog.avast.com/meet-adylkuzz-cryptocurrency-

mining-malware-spreading-using-the-same-exploit-as-wannacry, acedido em 2019/01/29.
33. Kudo, Y.: Trojan.Adylkuzz (2017), https://www.symantec.com/security-center/writeup/2017-051707-0237-99?tabid=2, acedido em 2019/01/26.
34. Kuzin, M., Shmelev, Y. e Galov, D.: SambaCry is coming (2017), https://securelist.com/sambacry-is-coming/78674, acedido em 2019/01/28.
35. Lau, H.: Browser-Based Cryptocurrency Mining Makes Unexpected Return from the Dead (2017), https://www.symantec.com/blogs/threat-intelligence/browser-mining-cryptocurrency, acedido em 2019/01/23.
36. Laura: XMRig Miner Trojan – How To Remove (2018), https://www.2-viruses.com/remove-xmrig-miner-trojan, acedido em 2019/01/22.
37. Laya, P.: Venezuela's Collapse (2019), https://www.bloomberg.com/quicktake/venezuela-price-revolution, acedido em 2019/01/25.
38. Hurley, J. e Chen, J.: Proceedings of the 13th International Conference on Cyber Warfare and Security (ICCWS 2018). National Defense University Washington DC, USA (2018).
39. Li, P., Salour, M., Su, X.: Survey of Internet Worm Detection and Containment. The Electronic Magazine of Original Peer-Reviewed Survey Articles, Vol. 10, N. 1, 20-35 (2008).
40. Lopatin, E.: Kaspersky Security Bulletin 2018 – Story of the year – Miners (2018), https://securelist.com/kaspersky-security-bulletin-2018-story-of-the-year-miners/89096, acedido em 2018/12/23.
41. Marr, B.: A Very Brief History Of Blockchain Technology Everyone Should Read (2018), https://www.forbes.com/sites/bernardmarr/2018/02/16/a-very-brief-history-of-blockchain-technology-everyone-should-read/#4d7cc2a37bc4, acedido em 2019/01/16.
42. Marr, B.: The 5 Big Problems With Blockchain Everyone Should Be Aware Of (2018a), https://www.forbes.com/sites/bernardmarr/2018/02/19/the-5-big-problems-with-blockchain-everyone-should-be-aware-of/#59da16a31670, acedido em 2019/01/16.
43. McAfee: Threat Report – Don't Join Blockchain Revolution Without Ensuring Security. McAfee Labs Threats Report (2018).
44. Microsoft: Surface Pro (5.ª Geração) – Especificações Técnicas (2019), https://www.microsoft.com/pt-pt/p/surface-pro-5ª-geracao/8NKT9WTTRBJK, acedido em 2019/03/16.
45. Minerva Labs Research Team: WaterMiner – a New Evasive Crypto-Miner (2017), https://blog.minerva-labs.com/waterminer-a-new-evasive-crypto-miner, acedido em 2019/01/23.
46. Murray, M.: A Reuteurs Visual Guide – Blockchain explained (2017), http://graphics.reuters.com/TECHNOLOGY-BLOCKCHAIN/010070P11GN/index.html, acedido em 2018/12/18.
47. Mursch, T.: How to find cryptojacking malware (2018). https://badpackets.net/how-to-find-cryptojacking-malware, acedido em 2019/04/14.
48. Neghaiwi, B.: Swiss startup SEBA raises funds to build crypto bank (2018), https://www.reuters.com/article/us-swiss-seba/swiss-startup-seba-raises-funds-to-build-crypto-bank-idUSKCN1M635O, acedido em 2018/12/19.
49. Newman, L.: Your Browser Could Be Mining Cryptocurrency For A Stranger (2017), https://www.wired.com/story/cryptojacking-cryptocurrency-mining-browser, acedido em 2019/01/23.

50. Osborne, C.: Brutal cryptocurrency mining malware crashes your PC when discovered (2018), https://www.zdnet.com/article/brutal-cryptominer-crashes-your-pc-when-discovered, acedido em 2019/01/24.
51. Osborne, C.: Japan issues first-ever prison sentence in cryptojacking case (2018a), https://www.zdnet.com/article/for-the-first-time-remote-cryptojacker-sentenced-for-exploiting-coinhive, acedido em 2019/01/24.
52. Parreira, R.: Blockchain poderá promover contratos de trabalho inteligentes e eliminar intermediários (2018), https://tek.sapo.pt/noticias/negocios/artigos/blockchain-podera-promover-contratos-de-trabalho-inteligentes-e-eliminar-intermediarios, acedido em 2018/12/19.
53. Peck, M.: Blockchains – How They Work and Why They'll Change the World (2017), https://spectrum.ieee.org/computing/networks/blockchains-how-they-work-and-why-theyll-change-the-world, acedido em 17/03/2019.
54. Pinheiro, A., D'Espiney, J. e Barroso, R.: Venda de casas em bitcoins já chegou a Portugal (2018), https://www.dn.pt/dinheiro/interior/venda-de-casas-em-bitcoins--ja-chegou-a-portugal-9029355.html, acedido em 2018/11/27.
55. Rauchberger, J., Schrittwieser, S., Dam, T., Luh, R., Buhov, D., Pötzelsberger, G. e Kim, H.: The Other Side of the Coin: A Framework for Detecting and Analyzing Web-based Cryptocurrency Mining Campaigns. ARES 2018 – International Conference on Availability, Reliability and Security, 1-10 (2018).
56. Rodrigues, M.: Adylkuzz utiliza a mesma vulnerabilidade que o WannaCry para criar dinheiro digital (2017), https://observador.pt/2017/05/17/adylkuzz-utiliza-vulnerabilidade-do-wannacry-para-criar-dinheiro, acedido em 2019/01/29.
57. Rodriguez, J. e Posegga, J.: RAPID: Resource and API-Based Detection Against In-Browser Miners. Annual Computer Security Applications Conference – ACSAC '18, 313-326 (2018).
58. Rossow, A.: How Blockchain Technology Can Help Power A New 21st Century Metropolis (2018), https://www.forbes.com/sites/andrewrossow/2018/09/19/how-blockchain-technology-can-help-power-a-new-21st-century-metropolis/#55eb6e057d65, acedido em 2019/01/18.
59. Rutkowska, J.: Introducing Stealth Malware Taxonomy. COSEINC Advanced Malware Labs, v. 1.01, 1-9 (2006).
60. Sanabria, A.: Malware Analysis – Environment Design and Architecture. SANS Institute Information Security Reading Room (2007).
61. SAPO TEK: Máquina de criptomoedas chegou a Braga e pode estar a caminho de outras cidades (2018), https://tek.sapo.pt/noticias/computadores/artigos/maquina-de-criptomoedas-chegou-a-braga-e-pode-estar-a-caminho-de-outras-cidades, acedido em 2018/11/26.
62. Siciliano, R.: Hackers Are Evolving Faster Than Technology, https://www.thebalance.com/how-has-hacking-evolved-with-technological-advances-1947546, acedido em 2019/01/02.
63. Sikorski, M. e Honig, A.: Practical Malware Analysis – The Hands-On Guide to Dissecting Malicious Software. No Starch Press Inc., San Francisco, EUA (2012).
64. Suarez-Tangil, G., Tapiador, J., Peris-Lopez, P., Ribagorda, A.: Evolution, Detection and Analysis of Malware for Smart Devices, Vol. 16, II, 961-987 (2014).

65. Subrahmanian, V., Ovelgonne, M., Dumitras, T. e Praksh, B.: Types of Malware and Malware Distribution Strategies. The Global Cyber-Vulnerability Report, 33-46. Springer, Suiça (2015).
66. Suleiman, B. e Husain, R.: Study of Computer Malware and Its Taxonomy. International Journal of Engineering and Applied Sciences, ISSN 2394-3661, Vol. 2, Issue-8, 54-56 (2015).
67. Symantec: 2018 Internet Security Threat Report [ISTR], Vol. 23 (2018), https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-executive-summary-en.pdf, acedido em 2019/01/04.
68. Symantec: 2019 Internet Security Threat Report [ISTR], Vol. 24 (2019).
69. Tabone, S.: Cyber Security 51 Handy Things To Know About Cyber Attacks. CreateSpace Independent Publishing Plataform, California (2017).
70. Thomas, S. e Francillon, A.: Backdoors – Definition, Deniability and Detection. Proceedings of the 21st International Symposium on Research in Attacks, Intrusions and Defenses. Heraklion, Grécia (2018).
71. United States Computer Emergency Readiness Team (US-CERT): Security Tip – Defending Against Illicit Cryptocurrency Mining Activity (2018), https://www.us-cert.gov/ncas/tips/ST18-002, acedido em 2019/01/18.
72. Xie, M.: Bitcoin Mining Is More Popular And More Destructive Than Ever (2018), https://www.forbes.com/sites/forbestechcouncil/2018/05/24/bitcoin-mining-is-more-popular-and-more-destructive-than-ever/#5186db4d4f1f, acedido em 2018/12/20.
73. Yadav, H. e Gour, S.: Cyber Attacks – An impact on Economy to an organization. International Journal of Information & Computing Technology, ISSN 0974-2239, Vol. 4, Num. 9, 937-940 (2014).
74. Wappalyzer: Cryptominer (2019). https://www.wappalyzer.com/categories/cryptominer, acedido em 2019/04/20.
75. Wolfson, R.: Cryptojacking On The Rise: WebCobra Malware Uses Victims' Computers To Mine Cryptocurrency (2018), https://www.forbes.com/sites/rachelwolfson/2018/11/13/cryptojacking-on-the-rise-webcobra-malware-uses-victims-computers-to-mine-cryptocurrency, acedido em 2018/11/29.
76. WorldCoinIndex: Bitcoin Gráficos (2019), https://www.worldcoinindex.com/pt/Moeda/bitcoin, acedido em 2019/01/18.
77. WorldCoinIndex: Ethereum Gráficos (2019a), https://www.worldcoinindex.com/pt/Moeda/ethereum, acedido em 2019/01/18.
78. WorldCoinIndex: Monero Gráficos (2019b), https://www.worldcoinindex.com/pt/Moeda/monero, acedido em 2019/01/18.

Apêndice A – Constituição da amostra

Tabela n.º 8 – Amostra para teste, obtida pelo Publicwww, com a(s) restante(s) plataforma(s) sinalizadoras, e indicação de existência de aviso para a mineração no próprio site.

Tipo	N.º	Site	Notmining	Wappalyzer	Aviso
CoinHive	1	http://moonbit.co.in		X	
	2	http://seriesdanko.to		X	
	3	https://flaru.com			
	4	https://www.vidics.to		X	
	5	http://publishyourarticles.net		X	
	6	https://bestvseries.com	X	X	
	7	http://streamaclic.fr		X	
	8	http://laspalabras.net		X	
	9	http://site4business.net			
	10	http://www.bayimg.com		X	
	11	http://tubreveespacio.com		X	
	12	http://themelike.net		X	
	13	http://pixroute.com			
	14	http://zeenews.india.com			
	15	http://versuri-si-creatii.ro		X	
	16	http://getspacecloud.org		X	
	17	https://lyapidov.ru			
	18	https://108clip.com		X	
	19	http://www.wikiooz.ir	?	X	
	20	https://tutoriadroid.blogspot.com		X	
Crypto-Loot	21	http://ooo-radiocom.ru	X		
	22	http://legendaoficial.net		X	
	23	https://infoglaz.ru			
	24	http://acmeta.com	X		
	25	http://www.bebidaliberada.com.br			
	26	http://newspettacolo.com	X		
	27	http://cherry-market.ru	X		
	28	http://poliklinika72.ru	X		
	29	http://medicinarf.ru			
	30	https://cryptogears2018.myshopify.com			
	31	https://bitblitz.org			
	32	https://antmauditions.com	X	X	
	33	http://web.crictime.com			
	34	http://gtplsaathi.com			
	35	http://harborea.eu			
	36	http://gtpl.net	?	X	
	37	https://talawa.fr			
	38	http://designerslib.com	X		
	39	http://wuwow.tw			
	40	http://center-pmpk.ru	X	X	

CoinImp	41	http://uploadboy.me			
	42	http://fanserials.irish			
	43	http://graphic-dl.com			
	44	http://mamanema.com			
	45	http://paintballgames62.com			
	46	http://ua.kalkulilo.net			
	47	http://ccleaner.com			
	48	http://littlebyte.net			
	49	http://biser.info	X		
	50	https://tkg.af	X	X	
	51	http://www.insai.gob.ve			
	52	http://funnymama.com			
	53	http://madacademy.it	X	X	
	54	http://ventureplaza.net	X	X	
	55	http://tvrex.net	X	X*	
	56	http://uandblog.com			
	57	http://mp3song-s.com			
	58	http://onlineserieswatch.com			
	59	http://tutorial-reports.com			
	60	https://www.eonsmoke.com			
deepMiner	61	http://www.gailzavala.com	X		
	62	http://360eye.cc	X		
	63	https://www.fixinfectedpc.com			
	64	http://lqrsw.com	X		
	65	http://def18.com	X		
	66	https://colleencollection.com.au	X		
	67	http://double-sim.com	X		
	68	http://312752.top	X		
	69	http://lanchuangclub.com	X		
	70	http://atril.com			
	71	http://ioshi.net	X		
	72	http://beuyels.com	X		
	73	http://www.leemc.cn	X		
	74	http://weightlo.com	X		
	75	http://mumineendownloads.com	X		
	76	http://inrebus.com		X	
	77	http://1365kk.com	X		
	78	http://web.archieve.org			
	79	http://vitalivf.com	X	X	
	80	http://epichappybirthdaysongs.com		X	
JSEcoin	81	http://hq-pictures.com	X	X	X
	82	https://songspk.mobi	X	X	X
	83	http://ciberpeliculashd.net	X	X	X
	84	https://coinmarketcal.com			
	85	https://crisanimex.com	X	X	X
	86	https://www.fbdown.me			
	87	https://canalpelis.com	X		
	88	http://only-soft.org			
	89	https://csubakka.hu	X	X	X
	90	http://alinafaucet.win	?	X	
	91	http://viraltecoop.com			
	92	https://arabbit.net			
	93	http://claimulike.win	X	X	
	94	https://sonyoutube.com	X	X	X
	95	http://pelisfull.tv	X	X	X
	96	http://episode24.pl			
	97	http://gametracker.rs			
	98	http://nemkacsa.com	X		
	99	http://socks24.org	X	X	X
	100	http://fans.bz	X	X	

Legenda: ? – Apenas contém um alerta;

***** – Identifica um tipo de *cryptojacking* diferente do referido.

Apêndice B – Resultados dos testes à amostra

Tabela n.º 9 – Valores obtidos para os quatro testes realizados a cada um dos 100 sites da amostra.

N.º	*Browser*	SO	$\%CPU_{máx}$	$\%CPU_{mín}$	$\%CPU_{m}$	$\%GPU_{máx}$	$\%GPU_{mín}$	$\%GPU_{m}$	Tf_{c}	v_{m}
1	Chrome	W	100,00	35,64	45,83	13,38	1,47	2,29	69,50	81,92
		A	100,00	9,94	62,25	8,64	0,97	4,59	74,00	658,54
	Firefox	W	59,43	10,24	23,04	2,52	0,68	1,30	69,00	5,32
		L	65,32	9,09	20,38	7,97	1,04	1,70	56,50	34,80
	Média		81,19	16,23	37,88	8,13	1,04	2,47	67,25	195,14
2	Chrome	W	64,11	0,08	9,71	5,84	0,17	0,84	55,00	5980,16
		A	32,89	0,49	2,94	5,42	0,20	0,64	43,00	3,69
	Firefox	W	28,27	1,27	5,64	1,63	0,16	0,40	52,00	5,75
		L	66,84	0,93	6,72	2,89	0,18	0,39	36,50	395,81
	Média		48,03	0,69	6,25	3,95	0,18	0,57	46,63	1596,35
3	Chrome	W	49,29	24,71	26,62	1,03	0,06	0,16	61,50	3,41
		A	25,49	0,00	1,23	3,28	0,18	0,37	43,00	1,77
	Firefox	W	52,41	0,59	8,99	9,55	0,16	0,42	49,50	6,25
		L	12,51	0,83	3,68	1,49	0,18	0,27	36,50	7,01
	Média		34,93	6,53	10,13	3,84	0,15	0,31	47,63	4,61
4	Chrome	W	30,17	0,00	1,84	1,94	0,15	0,32	43,50	1,61
		A	37,16	0,00	1,79	4,43	0,18	0,37	40,00	0,64
	Firefox	W	31,32	0,59	5,59	2,58	0,17	0,37	48,50	5,00
		L	45,83	1,13	4,97	2,42	0,18	0,30	34,50	18,80
	Média		36,12	0,43	3,55	2,84	0,17	0,34	41,63	6,52
5	Chrome	W	85,61	0,00	13,14	11,23	0,06	0,67	53,50	21,51
		A	37,17	0,00	2,12	4,40	0,17	0,32	40,00	0,47
	Firefox	W	18,47	0,92	5,81	4,24	0,14	0,39	40,50	12,51
		L	42,65	1,16	5,56	2,08	0,17	0,28	36,50	9,92
	Média		45,98	0,52	6,66	5,49	0,14	0,42	42,63	11,10
6	Chrome	W	10,24	0,49	3,62	0,99	0,16	0,31	47,00	4,08
		A	58,65	1,64	4,70	5,20	0,05	0,27	41,00	17,73
	Firefox	W	67,14	2,18	8,23	6,91	0,21	0,51	45,00	18,64
		L	65,32	3,69	8,16	2,53	0,17	0,34	36,50	32,60
	Média		50,34	2,00	6,18	3,91	0,15	0,36	42,38	18,26
7	Chrome	W	29,32	0,24	5,19	1,12	0,15	0,31	48,00	5,87
		A	29,58	0,00	2,54	3,72	0,18	0,40	43,00	2,48
	Firefox	W	60,60	1,27	7,91	3,48	0,25	0,47	45,00	9,40
		L	30,97	2,32	7,01	2,43	0,18	0,38	40,50	11,18
	Média		37,62	0,96	5,66	2,69	0,19	0,39	44,13	7,23

8	Chrome	W	36,84	0,00	2,99	3,56	0,16	0,41	45,00	6,27
		A	29,40	0,00	1,58	3,26	0,10	0,35	40,00	2,91
	Firefox	W	31,80	1,66	5,66	11,24	0,25	0,47	46,00	3,11
		L	22,29	0,53	3,69	1,55	0,15	0,27	38,50	6,04
	Média		30,08	0,55	3,48	4,90	0,17	0,38	42,38	4,58
9	Chrome	W	39,15	0,08	3,99	15,43	0,14	0,54	48,50	10,04
		A	47,74	0,00	2,02	4,75	0,21	0,44	40,00	8,49
	Firefox	W	14,17	1,24	4,92	2,97	0,13	0,43	41,50	3,11
		L	49,68	0,77	4,03	2,70	0,17	0,30	35,00	8,75
	Média		37,69	0,52	3,74	6,46	0,16	0,43	41,25	7,60
10	Chrome	W	70,35	24,25	27,01	1,08	0,13	0,25	59,50	8,17
		A	23,97	0,00	1,75	3,62	0,11	0,37	38,50	2,07
	Firefox	W	51,00	2,01	5,54	1,42	0,25	0,40	50,00	1,73
		L	41,49	1,32	5,06	1,99	0,17	0,27	34,50	14,06
	Média		46,70	6,90	9,84	2,03	0,17	0,32	45,63	6,51
11	Chrome	W	37,98	0,13	9,58	14,08	0,12	0,82	40,00	8,26
		A	24,69	0,00	2,56	4,86	0,13	0,37	40,50	1,17
	Firefox	W	38,19	1,70	6,36	2,65	0,25	0,44	45,50	6,98
		L	62,55	2,20	7,45	4,59	0,09	0,34	35,00	33,06
	Média		40,85	1,01	6,49	6,55	0,15	0,49	40,25	12,36
12	Chrome	W	83,77	0,14	25,43	1,48	0,12	0,25	65,50	8,28
		A	30,62	0,00	1,71	5,83	0,10	0,34	39,00	2,65
	Firefox	W	73,08	0,93	28,24	4,30	0,24	0,52	66,50	12,64
		L	22,75	0,58	3,73	3,57	0,17	0,29	36,50	7,99
	Média		52,56	0,41	14,78	3,80	0,16	0,35	51,88	7,89
13	Chrome	W	53,58	24,32	26,79	0,55	0,10	0,22	58,50	4,26
		A	36,38	0,00	1,25	3,83	0,19	0,36	42,00	1,53
	Firefox	W	11,85	0,96	5,44	4,21	0,24	0,42	49,00	4,06
		L	17,93	0,43	3,65	3,01	0,17	0,29	36,50	9,06
	Média		29,94	6,43	9,28	2,90	0,18	0,32	46,50	4,73
14	Chrome	W	57,09	2,86	10,89	13,52	0,15	0,59	55,00	6,12
		A	71,52	0,48	6,89	6,18	0,17	0,50	43,00	32,78
	Firefox	W	72,30	0,14	6,98	6,97	0,24	0,58	53,50	15,53
		L	63,72	3,57	12,93	8,38	0,16	0,51	39,50	197,69
	Média		66,16	1,76	9,42	8,76	0,18	0,55	47,75	63,03
15	Chrome	W	63,33	0,19	7,42	5,76	0,13	0,38	48,00	6,07
		A	39,16	0,00	2,05	3,87	0,11	0,32	40,50	2,58
	Firefox	W	35,24	0,53	5,96	2,37	0,25	0,45	48,00	28,64
		L	58,27	4,17	11,75	2,22	0,15	0,35	46,00	52,76
	Média		49,00	1,22	6,80	3,56	0,16	0,38	45,63	22,51

16	Chrome	W	86,35	0,00	6,56	3,52	0,16	0,38	46,00	6,23
		A	36,39	0,00	1,46	3,19	0,19	0,37	37,50	3,06
	Firefox	W	65,28	0,92	7,13	7,66	0,25	0,68	48,50	19,08
		L	48,52	1,13	6,48	2,09	0,17	0,29	41,00	21,49
	Média		59,14	0,51	5,41	4,12	0,19	0,43	43,25	12,47
17	Chrome	W	64,34	0,00	5,34	4,07	0,16	0,36	46,50	7,67
		A	48,88	0,00	2,05	5,39	0,15	0,43	40,00	8,27
	Firefox	W	27,83	1,37	6,90	2,41	0,25	0,57	48,00	7,66
		L	60,34	3,47	7,96	2,84	0,16	0,30	41,50	12,80
	Média		50,35	1,21	5,56	3,68	0,18	0,42	44,00	9,10
18	Chrome	W	58,61	6,34	12,08	18,51	0,66	1,16	51,00	3,53
		A	97,64	23,96	36,28	7,33	2,86	3,86	62,00	6,89
	Firefox	W	33,36	12,23	19,21	9,65	1,01	1,44	55,50	15,18
		L	39,93	1,46	6,87	3,38	0,17	0,33	40,00	30,44
	Média		57,39	11,00	18,61	9,72	1,18	1,70	52,13	14,01
19	Chrome	W	41,10	5,19	17,32	8,03	0,07	0,30	45,00	6,85
		A	66,88	1,79	16,26	6,57	0,58	1,48	48,50	249,24
	Firefox	W	39,93	4,82	13,08	6,89	0,25	0,60	51,50	153,57
		L	71,91	3,22	14,31	2,33	0,15	0,55	40,50	438,87
	Média		54,96	3,76	15,24	5,96	0,26	0,73	46,38	212,13
20	Chrome	W	32,11	0,00	4,18	14,70	0,07	0,42	43,00	4,49
		A	39,49	0,00	2,26	4,05	0,18	0,40	38,50	2,22
	Firefox	W	36,40	1,67	10,01	15,22	0,27	0,73	46,50	8,04
		L	49,32	2,63	7,95	2,46	0,16	0,31	38,00	213,65
	Média		39,33	1,08	6,10	9,11	0,17	0,47	41,50	57,10
21	Chrome	W	62,95	1,70	10,96	6,16	0,14	0,43	50,00	8,51
		A	49,66	0,00	9,49	5,62	0,18	0,81	41,00	3,05
	Firefox	W	29,81	0,88	6,55	1,40	0,25	0,39	48,00	6,73
		L	57,21	1,77	7,91	1,12	0,16	0,25	40,50	12,63
	Média		49,91	1,09	8,73	3,58	0,18	0,47	44,88	7,73
22	Chrome	W	78,16	0,14	12,83	3,24	0,13	0,64	60,50	232,28
		A	81,67	1,66	11,62	6,51	0,15	0,59	45,50	407,92
	Firefox	W	64,11	2,48	10,56	7,56	0,26	1,01	46,00	50,76
		L	59,02	1,99	25,29	2,68	0,16	1,06	60,00	116,37
	Média		70,74	1,57	15,08	5,00	0,18	0,83	53,00	201,83
23	Chrome	W	59,98	0,00	6,32	3,40	0,13	0,40	46,00	4,82
		A	73,87	0,87	5,77	4,90	0,42	0,87	40,50	86,10
	Firefox	W	82,06	1,70	9,20	7,89	0,25	0,81	45,50	46,16
		L	65,70	2,69	9,74	8,64	0,19	0,50	39,50	41,07
	Média		70,40	1,32	7,76	6,21	0,25	0,65	42,88	44,54

24	Chrome	W	30,95	0,00	6,35	2,51	0,06	0,32	45,00	6,07
		A	36,77	0,00	1,86	6,24	0,19	0,39	46,50	2,06
	Firefox	W	53,58	1,35	8,05	2,87	0,25	0,48	46,00	570,17
		L	15,91	0,83	5,62	1,60	0,17	0,26	36,50	7,21
	Média		34,30	0,55	5,47	3,31	0,17	0,36	43,50	146,38
25	Chrome	W	80,50	0,14	7,96	2,59	0,37	0,14	46,50	128,71
		A	69,18	0,00	4,61	7,77	0,15	0,56	39,00	249,23
	Firefox	W	53,58	2,09	7,38	9,43	0,25	0,59	48,00	87,74
		L	64,13	3,01	9,15	3,45	0,15	0,35	39,50	298,84
	Média		66,85	1,31	7,28	5,81	0,23	0,41	43,25	191,13
26	Chrome	W	77,38	0,00	12,79	27,14	0,18	1,06	49,50	11,10
		A	70,68	0,00	15,97	8,15	0,18	1,55	41,00	68,20
	Firefox	W	68,39	1,77	10,63	9,50	0,09	0,81	42,50	100,21
		L	58,27	1,70	15,71	3,08	0,17	0,76	41,50	41,53
	Média		68,68	0,87	13,78	11,97	0,16	1,05	43,63	55,26
27	Chrome	W	72,30	0,00	14,12	6,78	0,20	0,81	54,00	12,90
		A	64,12	0,00	11,59	10,66	0,10	1,33	57,50	1,28
	Firefox	W	36,75	0,88	8,11	2,66	0,25	0,79	45,50	8,58
		L	39,56	0,99	11,50	1,95	0,18	0,64	37,50	59,68
	Média		53,18	0,47	11,33	5,51	0,18	0,89	48,63	20,61
28	Chrome	W	31,37	0,00	2,50	6,97	0,14	0,43	42,00	5,81
		A	31,76	0,00	1,94	6,08	0,19	0,38	40,50	2,44
	Firefox	W	17,69	2,03	5,96	2,99	0,25	0,44	45,50	5,33
		L	19,67	1,53	5,69	1,46	0,17	0,27	35,00	19,19
	Média		25,12	0,89	4,02	4,38	0,19	0,38	40,75	8,19
29	Chrome	W	90,49	0,00	9,79	4,12	0,17	0,55	43,00	69,46
		A	78,55	0,48	22,56	14,11	0,14	0,59	59,50	17,97
	Firefox	W	36,78	1,31	6,82	1,06	0,17	0,42	43,00	57,95
		L	43,84	3,23	8,20	2,29	0,17	0,34	39,00	20,56
	Média		62,42	1,26	11,84	5,40	0,16	0,48	46,13	41,49
30	Chrome	W	62,52	0,14	12,57	5,04	0,08	0,65	59,00	3,59
		A	7,87	0,00	1,36	1,66	0,18	0,34	36,50	1,35
	Firefox	W	24,68	1,70	8,83	11,07	0,26	1,40	52,00	6,30
		L	60,61	0,75	11,92	2,72	0,18	0,67	39,00	24,83
	Média		38,92	0,65	8,67	5,12	0,18	0,77	46,63	9,02
31	Chrome	W	86,88	0,14	10,66	4,32	0,05	0,50	46,50	59,90
		A	17,66	0,00	1,40	10,72	0,18	0,41	39,00	3,04
	Firefox	W	49,66	0,00	14,24	1,41	0,17	0,48	50,50	475,99
		L	11,43	1,14	5,28	1,51	0,09	0,27	36,00	62,18
	Média		41,41	0,32	7,90	4,49	0,12	0,42	43,00	150,28

32	Chrome	W	75,03	0,00	9,20	1,21	0,14	0,36	39,50	24,13
		A	34,47	0,00	2,04	8,41	0,11	0,41	38,00	5,19
	Firefox	W	47,01	1,39	6,10	8,44	0,16	0,63	45,00	15,34
		L	62,16	0,35	4,90	1,62	0,16	0,28	40,00	15,34
	Média		54,67	0,44	5,56	4,92	0,14	0,42	40,63	15,00
33	Chrome	W	6,55	0,00	34,07	1,20	0,07	0,31	40,00	3,62
		A	31,79	0,00	2,11	12,74	0,15	0,49	38,50	6,85
	Firefox	W	78,28	1,73	19,54	10,83	0,25	0,66	49,00	88,10
		L	15,15	1,21	4,88	6,27	0,09	0,35	41,50	3,34
	Média		32,94	0,74	15,15	7,76	0,14	0,45	42,25	25,48
34	Chrome	W	30,95	0,00	5,32	1,00	0,14	0,33	41,50	4,15
		A	25,44	0,00	1,24	4,34	0,18	0,37	36,50	1,46
	Firefox	W	34,20	1,70	6,24	2,88	0,25	0,51	45,50	20,53
		L	14,93	1,21	4,32	1,77	0,08	0,28	36,50	2,76
	Média		26,38	0,73	4,28	2,50	0,16	0,37	40,00	7,22
35	Chrome	W	69,93	0,14	10,67	5,41	0,14	0,62	42,00	169,42
		A	61,77	0,08	13,74	25,46	0,19	1,48	43,00	217,50
	Firefox	W	45,37	1,28	9,18	3,13	0,26	0,85	45,50	175,33
		L	56,31	1,40	10,68	2,73	0,17	0,61	37,00	248,63
	Média		58,35	0,73	11,07	9,18	0,19	0,89	41,88	202,72
36	Chrome	W	54,47	0,49	7,91	3,41	0,16	0,67	51,50	61,11
		A	64,15	0,00	10,31	6,32	0,18	1,13	40,50	70,95
	Firefox	W	36,05	0,00	2,05	1,42	0,17	0,34	51,00	4,50
		L	95,71	1,19	14,07	2,50	0,17	0,62	50,50	288,69
	Média		62,60	0,42	8,59	3,41	0,17	0,69	48,38	106,31
37	Chrome	W	32,12	0,00	3,52	13,28	0,09	0,41	39,50	8,94
		A	32,16	0,00	1,98	5,69	0,19	0,37	39,00	1,65
	Firefox	W	19,29	0,00	2,56	6,85	0,13	0,41	44,00	9,01
		L	15,29	1,62	5,09	1,21	0,17	0,28	38,00	4,78
	Média		24,72	0,41	3,29	6,76	0,15	0,37	40,13	6,09
38	Chrome	W	56,66	0,00	7,02	1,18	0,14	0,30	46,00	7,26
		A	64,54	0,00	3,51	21,26	0,19	0,67	39,50	5,00
	Firefox	W	33,32	0,00	2,22	2,04	0,16	0,35	41,50	5,56
		L	61,77	1,64	8,11	3,31	0,15	0,34	36,50	15,11
	Média		54,07	0,41	5,22	6,95	0,16	0,42	40,88	8,23
39	Chrome	W	37,22	0,00	1,95	4,11	0,18	0,38	43,50	5,47
		A	73,08	0,00	13,14	8,79	0,19	1,33	42,00	105,44
	Firefox	W	58,65	0,49	7,24	2,49	0,19	0,72	43,50	11,06
		L	54,75	1,74	12,55	3,82	0,17	0,77	40,00	61,82
	Média		55,93	0,56	8,72	4,80	0,18	0,80	42,25	45,95

40	Chrome	W	85,96	0,00	9,17	4,08	0,13	0,50	44,00	72,11
		A	33,29	0,00	2,70	10,36	0,17	0,57	39,50	5,16
	Firefox	W	40,71	0,14	10,74	1,83	0,16	0,39	43,00	11,47
		L	45,39	1,13	12,65	9,33	0,16	0,33	50,50	119,72
	Média		51,34	0,32	8,82	6,40	0,16	0,45	44,25	52,11
41	Chrome	W	40,32	0,00	4,58	1,01	0,18	0,44	47,00	312,88
		A	30,56	0,00	1,31	6,50	0,19	0,41	41,50	1,47
	Firefox	W	14,14	0,00	2,05	1,90	0,10	0,34	41,00	2,04
		L	37,76	1,01	4,08	0,48	0,16	0,25	34,50	5,40
	Média		30,70	0,25	3,01	2,47	0,16	0,36	41,00	80,45
42	Chrome	W	64,11	0,08	17,11	11,18	0,09	0,40	57,50	11,20
		A	44,61	0,00	1,74	5,03	0,18	0,40	42,00	6,23
	Firefox	W	21,59	1,26	5,00	2,10	0,15	0,37	43,50	2,65
		L	29,40	2,01	6,25	2,29	0,17	0,30	35,50	21,47
	Média		39,93	0,84	7,53	5,15	0,15	0,37	44,63	10,39
43	Chrome	W	57,09	0,53	5,57	4,37	0,11	0,34	44,50	8,21
		A	39,55	0,00	1,55	7,99	0,18	0,42	41,50	2,45
	Firefox	W	23,55	0,00	2,07	1,75	0,16	0,36	42,00	3,42
		L	42,27	0,04	4,15	10,38	0,17	0,31	36,50	5,68
	Média		40,62	0,14	3,34	6,12	0,16	0,36	41,13	4,94
44	Chrome	W	69,18	5,74	47,32	7,08	0,08	1,05	72,00	159,38
		A	79,33	49,67	55,39	17,27	0,13	1,44	68,00	361,44
	Firefox	W	75,46	49,72	55,03	4,82	0,13	0,75	67,50	139,76
		L	71,55	50,07	55,11	3,12	0,14	0,86	66,00	45,56
	Média		73,88	38,80	53,21	8,07	0,12	1,03	68,38	176,53
45	Chrome	W	92,59	50,17	56,88	7,28	0,13	0,87	73,00	28,97
		A	43,46	0,00	4,30	18,13	0,16	0,94	43,00	1,63
	Firefox	W	64,50	50,12	55,62	2,44	0,15	0,96	69,50	4,30
		L	19,25	1,03	5,41	2,23	0,17	0,26	41,00	3,59
	Média		54,95	25,33	30,55	7,52	0,15	0,76	56,63	9,62
46	Chrome	W	30,21	0,00	3,49	3,15	0,17	0,31	47,50	7,49
		A	20,76	0,00	2,14	3,59	0,18	0,38	36,00	3,97
	Firefox	W	26,74	0,00	5,78	2,28	0,15	0,37	49,50	3,09
		L	50,02	1,90	6,32	2,33	0,17	0,30	36,50	12,44
	Média		31,93	0,48	4,43	2,84	0,17	0,34	42,38	6,75
47	Chrome	W	51,01	0,00	7,76	3,95	0,14	0,47	42,00	31,01
		A	32,90	0,00	1,51	4,74	0,18	0,37	39,00	1,85
	Firefox	W	28,61	0,53	5,40	2,76	0,08	0,28	42,00	2,40
		L	53,62	1,54	8,10	12,29	0,19	0,49	41,00	8,39
	Média		41,54	0,52	5,69	5,94	0,15	0,40	41,00	10,91

48	Chrome	W	31,12	0,00	2,41	1,72	0,16	0,37	39,50	11,61
		A	55,56	0,00	7,09	6,53	0,17	0,81	59,00	1,42
	Firefox	W	11,10	0,14	3,19	1,57	0,18	0,31	40,50	1,76
		L	9,00	0,14	3,54	1,44	0,16	0,26	33,50	5,68
	Média		26,70	0,07	4,06	2,82	0,17	0,44	43,13	5,12
49	Chrome	W	16,99	2,15	28,61	6,61	0,15	0,70	49,00	86,93
		A	77,38	3,26	29,70	22,62	0,62	1,57	63,00	43,87
	Firefox	W	71,13	1,70	23,92	2,55	0,14	0,42	47,50	59,38
		L	68,80	2,95	25,51	4,38	0,13	0,45	54,50	74,96
	Média		58,58	2,52	26,94	9,04	0,26	0,79	53,50	66,29
50	Chrome	W	75,47	1,32	34,29	5,60	0,14	0,76	67,50	267,92
		A	68,79	19,64	43,31	7,77	0,14	0,84	60,00	201,27
	Firefox	W	61,38	27,05	41,09	1,81	0,13	0,47	61,00	148,38
		L	64,89	25,96	43,07	3,15	0,13	0,79	62,50	197,05
	Média		67,63	18,49	40,44	4,58	0,14	0,72	62,75	203,66
51	Chrome	W	70,35	0,04	12,34	4,78	0,15	1,05	44,50	137,63
		A	72,30	0,00	6,60	5,60	0,19	0,71	44,50	46,51
	Firefox	W	49,92	0,53	6,32	4,46	0,18	0,52	40,00	24,12
		L	68,00	1,22	9,91	11,28	0,17	0,63	41,50	124,91
	Média		65,14	0,45	8,79	6,53	0,17	0,73	42,63	83,29
52	Chrome	W	30,60	0,00	3,50	2,34	0,15	0,40	42,50	10,17
		A	52,82	0,00	1,67	6,30	0,18	0,41	42,50	1,98
	Firefox	W	10,71	0,00	1,97	2,12	0,19	0,37	41,00	1,73
		L	66,06	3,17	31,03	3,03	0,24	1,46	60,50	110,12
	Média		40,05	0,79	9,54	3,45	0,19	0,66	46,63	31,00
53	Chrome	W	77,77	42,27	52,77	5,92	0,12	0,83	71,00	220,28
		A	68,76	0,00	37,05	7,39	0,06	0,89	73,50	98,87
	Firefox	W	95,35	41,88	49,60	4,80	0,14	0,53	69,00	169,27
		L	73,94	42,27	52,20	9,56	0,13	0,88	69,00	218,06
	Média		78,96	31,61	47,91	6,92	0,11	0,78	70,63	176,62
54	Chrome	W	55,14	45,10	48,57	1,56	0,12	0,27	71,00	6,65
		A	54,87	46,11	48,70	0,75	0,14	0,23	71,50	2,40
	Firefox	W	65,67	46,17	48,76	6,21	0,13	0,35	71,50	3,22
		L	59,04	41,93	49,05	2,11	0,14	0,25	68,00	7,61
	Média		58,68	44,83	48,77	2,66	0,13	0,28	70,50	4,97
55	Chrome	W	11,41	0,89	5,11	0,98	0,09	0,32	44,00	12,52
		A	73,47	0,00	4,33	16,99	0,18	0,63	46,00	114,81
	Firefox	W	61,77	0,47	5,17	3,84	0,15	0,42	43,00	29,45
		L	62,94	0,73	6,26	8,85	0,16	0,39	42,50	30,07
	Média		52,40	0,52	5,22	7,67	0,15	0,44	43,88	46,71

56	Chrome	W	93,34	50,07	56,22	21,14	0,13	0,48	70,00	88,41
		A	58,26	49,72	51,66	1,98	0,12	0,28	71,00	2,68
	Firefox	W	59,82	50,07	51,47	2,15	0,13	0,27	71,00	5,74
		L	75,84	50,07	51,87	2,75	0,18	0,26	71,00	1158,56
	Média		71,82	49,98	52,81	7,01	0,14	0,32	70,75	313,85
57	Chrome	W	24,35	0,00	4,58	2,56	0,08	0,25	46,00	8,58
		A	54,45	1,35	20,44	4,46	0,06	0,34	79,50	5,23
	Firefox	W	68,01	0,48	46,04	1,93	0,14	0,31	50,00	4,59
		L	67,98	49,33	51,84	10,36	0,08	0,28	68,50	15,11
	Média		53,70	12,79	30,73	4,83	0,09	0,30	61,00	8,37
58	Chrome	W	69,57	2,05	11,47	6,95	0,15	0,40	47,50	14,51
		A	44,76	0,78	4,35	3,54	0,17	0,37	39,50	1,68
	Firefox	W	21,23	0,00	2,42	1,95	0,14	0,36	43,50	4,85
		L	56,31	0,44	4,76	13,09	0,15	0,34	39,50	9,56
	Média		47,97	0,82	5,75	6,38	0,15	0,37	42,50	7,65
59	Chrome	W	30,93	0,00	4,16	2,45	0,11	0,34	48,00	6,62
		A	36,82	1,19	4,71	4,27	0,17	0,36	38,00	2,45
	Firefox	W	20,06	0,00	2,46	4,37	0,17	0,39	42,00	3,07
		L	9,40	1,11	4,61	4,11	0,17	0,29	34,00	4,26
	Média		24,30	0,58	3,99	3,80	0,16	0,35	40,50	4,10
60	Chrome	W	67,61	31,40	41,07	2,09	0,22	0,46	70,50	19,42
		A	66,06	3,99	33,20	5,29	0,39	1,12	65,50	27,11
	Firefox	W	67,62	29,00	41,78	1,51	0,15	0,48	69,00	210,27
		L	76,60	13,40	42,65	14,55	0,15	0,63	64,00	110,26
	Média		69,47	19,45	39,68	5,86	0,23	0,67	67,25	91,76
61	Chrome	W	68,01	0,00	8,29	4,39	0,16	0,92	49,00	13,62
		A	n.d.	n.d.	n.d.	n.d.	n.d.	n.d.	n.d.	n.d.
	Firefox	W	53,24	0,47	31,52	0,82	0,14	0,37	59,00	9,67
		L	n.d.	n.d.	n.d.	n.d.	n.d.	n.d.	n.d.	n.d.
	Média		60,63	0,24	19,91	2,61	0,15	0,65	54,00	11,65
62	Chrome	W	50,46	0,00	4,75	4,45	0,17	0,48	45,00	6,98
		A	58,65	0,37	17,98	5,52	0,17	1,77	39,50	3,71
	Firefox	W	39,15	0,00	4,23	1,76	0,18	0,56	42,50	1,75
		L	59,43	30,95	35,40	2,13	1,24	1,40	65,00	166,10
	Média		51,92	7,83	15,59	3,47	0,44	1,05	48,00	44,63
63	Chrome	W	34,46	3,67	10,93	0,62	0,09	0,24	49,00	8,43
		A	64,11	2,42	10,19	6,60	0,16	0,39	45,00	28,46
	Firefox	W	40,71	5,37	9,00	2,68	0,93	1,19	45,50	3,12
		L	40,72	3,66	8,19	3,64	0,15	0,31	41,00	5,66
	Média		45,00	3,78	9,58	3,39	0,33	0,53	45,13	11,42

64	Chrome	W	52,02	0,00	11,70	5,18	0,07	0,84	53,50	28,59
		A	n.d.	n.d.	n.d.	n.d.	n.d.	n.d.	n.d.	n.d.
	Firefox	W	n.d.	n.d.	n.d.	n.d.	n.d.	n.d.	n.d.	n.d.
		L	n.d.	n.d.	n.d.	n.d.	n.d.	n.d.	n.d.	n.d.
	Média		52,02	0,00	11,70	5,18	0,07	0,84	53,50	28,59
65	Chrome	W	45,37	0,00	8,01	4,27	0,18	0,67	47,00	18,21
		A	57,60	1,19	11,62	5,15	0,17	1,08	39,00	2,25
	Firefox	W	33,27	0,00	5,44	2,46	0,19	0,75	42,50	19,83
		L	47,73	29,00	34,39	2,21	1,24	1,40	47,50	20,38
	Média		45,99	7,55	14,87	3,52	0,45	0,98	44,00	15,17
66	Chrome	W	30,56	0,00	3,85	6,44	0,16	0,45	44,00	3,93
		A	61,38	0,82	24,44	6,43	0,19	2,46	39,00	3,82
	Firefox	W	16,89	0,00	3,55	3,24	0,17	0,62	41,50	4,10
		L	48,12	1,68	33,63	1,96	0,18	1,36	46,00	9,58
	Média		39,24	0,63	16,37	4,52	0,18	1,22	42,63	5,36
67	Chrome	W	48,12	0,00	18,07	5,65	0,19	1,50	50,50	4,22
		A	63,72	17,82	38,38	6,89	2,71	3,89	59,50	2,97
	Firefox	W	35,24	0,00	9,12	2,66	0,18	1,30	41,50	3,36
		L	46,95	30,26	37,27	3,48	1,24	1,90	68,00	16,34
	Média		48,51	12,02	25,71	4,67	1,08	2,15	54,88	6,73
68	Chrome	W	45,00	1,69	8,73	1,97	0,15	0,39	51,00	3,97
		A	81,67	27,05	62,83	7,35	0,33	5,80	69,00	3,47
	Firefox	W	43,07	0,00	4,69	10,79	0,07	0,72	41,00	4,97
		L	46,95	31,34	38,49	9,01	1,20	1,51	63,50	10,99
	Média		54,17	15,02	28,69	7,28	0,44	2,11	56,13	5,85
69	Chrome	W	30,56	0,00	4,13	2,51	0,17	0,43	44,50	2,87
		A	15,57	0,43	3,27	0,96	0,17	0,29	40,00	1,96
	Firefox	W	22,37	0,00	2,89	2,56	0,19	0,44	42,00	32,56
		L	39,15	1,24	18,99	2,22	0,18	0,82	41,00	5,74
	Média		26,91	0,42	7,32	2,06	0,18	0,50	41,88	10,78
70	Chrome	W	49,27	1,30	15,92	2,79	0,15	0,58	51,50	18,07
		A	61,38	0,14	10,90	4,24	0,15	0,51	39,00	50,37
	Firefox	W	36,09	5,94	13,74	1,95	0,15	0,53	41,00	17,76
		L	63,76	5,99	14,60	18,64	0,16	0,65	53,00	40,81
	Média		52,63	3,34	13,79	6,91	0,15	0,57	46,13	31,75
71	Chrome	W	32,91	0,00	4,71	4,17	0,15	0,45	44,00	3,09
		A	62,16	1,05	19,23	10,74	0,16	2,54	36,00	4,49
	Firefox	W	22,74	0,00	3,47	2,72	0,16	0,43	38,00	7,48
		L	43,44	0,83	18,92	2,64	0,18	0,82	39,00	6,89
	Média		40,31	0,47	11,58	5,07	0,16	1,06	39,25	5,49

72	Chrome	W	59,04	2,81	19,27	3,77	0,16	0,95	53,50	83,43
		A	92,92	14,71	54,34	6,72	0,17	4,40	50,00	87,05
	Firefox	W	46,56	0,00	8,11	6,92	0,18	1,11	41,00	60,04
		L	57,48	34,47	40,97	3,54	1,26	1,81	65,50	83,39
	Média		64,00	13,00	30,67	5,24	0,44	2,07	52,50	78,48
73	Chrome	W	48,12	0,58	4,80	7,20	0,24	0,68	45,50	44,63
		A	19,66	3,61	6,92	2,34	0,37	0,77	38,50	4,24
	Firefox	W	52,41	0,00	7,26	3,08	0,10	0,79	42,00	99,07
		L	56,31	3,61	9,98	5,80	0,21	0,63	40,00	62,00
	Média		44,13	1,95	7,24	4,61	0,23	0,72	41,50	52,49
74	Chrome	W	59,04	0,20	10,47	1,77	0,18	0,52	56,50	8,82
		A	50,83	14,49	26,30	4,97	2,49	3,06	58,50	4,17
	Firefox	W	59,43	1,31	29,90	1,88	0,23	0,74	45,00	6,94
		L	n.d.	n.d.	n.d.	n.d.	n.d.	n.d.	n.d.	n.d.
	Média		56,43	5,33	22,22	2,87	0,97	1,44	53,33	6,65
75	Chrome	W	32,24	0,14	3,10	7,68	0,17	0,39	43,50	2,72
		A	38,94	0,85	3,56	4,49	0,18	0,34	40,00	5,49
	Firefox	W	27,41	0,00	2,20	1,76	0,16	0,34	41,00	1,10
		L	26,62	0,00	3,35	2,52	0,17	0,27	40,00	5,13
	Média		31,30	0,25	3,05	4,11	0,17	0,34	41,13	3,61
76	Chrome	W	34,10	0,88	4,48	8,42	0,16	0,37	46,00	3,55
		A	64,89	2,76	7,14	5,03	0,16	0,38	43,00	14,46
	Firefox	W	29,00	0,00	2,55	1,95	0,07	0,34	42,00	1,37
		L	59,43	5,08	12,58	9,83	0,38	0,79	40,00	48,75
	Média		46,86	2,18	6,69	6,31	0,19	0,47	42,75	17,03
77	Chrome	W	50,41	22,35	30,87	13,44	2,17	2,83	62,50	19,93
		A	72,69	46,56	63,23	8,64	3,84	5,51	69,50	38,18
	Firefox	W	44,09	8,29	15,39	4,13	1,87	2,34	50,50	30,27
		L	58,00	17,69	32,59	10,28	1,63	2,46	65,00	89,96
	Média		56,30	23,72	35,52	9,12	2,38	3,29	61,88	44,58
78	Chrome	W	18,47	0,00	2,83	2,05	0,17	0,33	44,50	3,75
		A	23,81	0,52	3,62	3,71	0,16	0,35	38,50	1,73
	Firefox	W	28,24	0,03	2,29	1,72	0,16	0,33	40,50	4,28
		L	11,34	0,93	3,82	0,45	0,17	0,25	36,50	4,99
	Média		20,47	0,37	3,14	1,98	0,17	0,32	40,00	3,69
79	Chrome	W	50,07	0,00	4,45	3,81	0,16	0,31	46,50	2,06
		A	59,62	1,01	9,88	5,32	0,16	0,37	42,50	5,52
	Firefox	W	24,33	0,00	1,83	2,31	0,18	0,33	41,50	2,67
		L	51,24	1,62	5,47	3,38	0,17	0,28	37,50	13,47
	Média		46,32	0,66	5,41	3,71	0,17	0,32	42,00	5,93

80	Chrome	W	60,60	0,00	4,26	13,13	0,17	0,44	42,00	19,64
		A	80,50	1,32	7,69	12,14	0,17	0,64	46,50	23,31
	Firefox	W	54,01	0,00	3,76	3,12	0,16	0,45	42,50	16,42
		L	9,29	0,72	3,96	2,04	0,17	0,25	35,50	8,43
	Média		51,10	0,51	4,92	7,61	0,17	0,45	41,63	16,95
81	Chrome	W	30,17	0,00	6,24	1,15	0,07	0,40	40,50	8,54
		A	69,18	1,58	7,20	6,42	0,16	0,51	40,00	93,05
	Firefox	W	33,70	12,04	18,40	1,99	1,18	1,59	47,50	4,47
		L	57,48	2,38	8,56	9,23	0,16	0,46	44,00	37,30
	Média		47,63	4,00	10,10	4,70	0,39	0,74	43,00	35,84
82	Chrome	W	80,11	2,48	24,24	14,95	0,15	1,72	47,50	409,60
		A	50,46	1,17	5,85	4,93	0,17	0,42	36,00	3,69
	Firefox	W	31,36	17,30	24,20	3,59	1,57	1,88	49,50	15,17
		L	34,86	0,44	4,90	2,18	0,17	0,31	35,50	12,33
	Média		49,20	5,35	14,80	6,41	0,52	1,08	42,13	110,20
83	Chrome	W	89,52	2,12	29,87	15,27	0,04	1,54	45,50	655,36
		A	61,03	0,52	14,58	5,32	0,17	0,66	39,00	11,63
	Firefox	W	21,57	3,65	10,87	3,00	0,08	0,39	49,50	5,58
		L	62,59	1,79	7,41	9,64	0,17	0,47	40,50	15,48
	Média		58,68	2,02	15,68	8,31	0,12	0,77	43,63	172,01
84	Chrome	W	92,92	42,32	57,10	17,90	3,36	4,04	72,00	19,77
		A	80,89	61,77	67,56	8,16	4,44	5,95	71,50	6,66
	Firefox	W	61,77	30,69	22,02	10,32	2,09	2,74	53,50	19,86
		L	80,13	52,02	64,40	8,52	1,81	3,28	75,00	83,24
	Média		78,93	46,70	52,77	11,23	2,93	4,00	68,00	32,38
85	Chrome	W	86,74	26,66	43,62	18,01	1,47	2,09	65,50	48,97
		A	96,15	51,29	66,63	14,81	4,31	6,10	70,50	221,43
	Firefox	W	65,28	9,89	18,35	6,37	1,22	1,89	42,50	7,78
		L	58,04	2,31	11,18	8,24	0,16	0,53	40,00	188,38
	Média		76,55	22,54	34,95	11,86	1,79	2,65	54,63	116,64
86	Chrome	W	54,84	0,00	6,73	3,71	0,08	0,33	45,50	15,81
		A	36,16	0,52	3,41	4,24	0,04	0,21	43,00	6,00
	Firefox	W	12,86	0,00	2,15	2,16	0,19	0,39	36,50	3,39
		L	42,66	0,14	5,90	0,94	0,17	0,35	37,00	389,41
	Média		36,63	0,17	4,55	2,76	0,12	0,32	40,50	103,65
87	Chrome	W	44,98	2,09	17,43	3,43	0,20	1,17	48,50	2,16
		A	74,25	61,77	66,78	6,50	5,44	5,95	71,50	11,57
	Firefox	W	44,63	2,09	11,30	3,62	0,18	1,00	48,50	5,40
		L	57,87	29,00	40,20	3,59	1,23	1,79	66,50	5,66
	Média		55,43	23,74	33,93	4,29	1,76	2,48	58,75	6,20

88	Chrome	W	39,99	0,00	2,96	4,16	0,16	0,40	43,00	2,14
		A	43,09	0,00	4,14	4,68	0,17	0,35	40,00	7,79
	Firefox	W	20,04	0,00	2,54	1,22	0,06	0,22	40,00	2,82
		L	40,70	0,04	5,70	7,55	0,17	0,41	36,50	32,12
	Média		35,96	0,01	3,84	4,40	0,14	0,35	39,88	11,22
89	Chrome	W	65,67	31,28	38,55	6,38	2,31	2,82	60,50	3,42
		A	33,77	0,91	4,56	5,10	0,14	0,39	37,50	7,53
	Firefox	W	17,91	1,71	6,68	3,05	0,16	0,37	42,50	3,90
		L	58,26	0,83	6,90	24,69	0,17	0,48	30,00	41,72
	Média		43,90	8,68	14,17	9,81	0,70	1,02	42,63	14,15
90	Chrome	W	71,91	23,62	30,79	5,33	2,06	2,64	67,50	25,34
		A	25,31	0,83	4,27	2,70	0,08	0,35	36,50	5,11
	Firefox	W	28,61	1,35	12,44	3,18	0,18	1,17	45,00	5,81
		L	11,72	0,83	3,74	3,04	0,18	0,28	33,00	3,08
	Média		34,39	6,66	12,81	3,56	0,63	1,11	45,50	9,84
91	Chrome	W	21,20	0,00	2,80	8,77	0,16	0,47	47,00	3,40
		A	36,39	1,21	5,62	4,57	0,09	0,42	37,00	8,86
	Firefox	W	12,61	0,00	2,72	2,21	0,18	0,46	40,50	3,80
		L	40,71	0,93	6,05	0,82	0,07	0,25	34,00	8,79
	Média		27,73	0,54	4,30	4,09	0,13	0,40	39,63	6,21
92	Chrome	W	74,40	4,01	20,43	13,45	0,14	0,95	56,00	120,07
		A	63,37	7,94	36,24	5,31	0,15	0,49	45,50	67,98
	Firefox	W	54,74	0,48	8,98	4,87	0,15	0,69	50,00	62,92
		L	55,92	6,78	14,70	2,03	0,15	0,41	43,00	11,03
	Média		62,11	4,80	20,09	6,42	0,15	0,64	48,63	65,50
93	Chrome	W	79,44	21,59	31,43	5,38	1,57	2,19	61,50	127,99
		A	37,27	0,82	3,67	5,07	0,16	0,34	36,50	1,14
	Firefox	W	52,00	5,24	19,03	3,53	0,09	1,24	40,00	44,55
		L	12,49	0,83	3,92	1,13	0,08	0,17	34,50	4,96
	Média		45,30	7,12	14,51	3,78	0,48	0,99	43,13	44,66
94	Chrome	W	73,48	25,88	33,46	7,20	1,91	2,59	65,50	119,65
		A	84,01	22,73	38,38	8,25	2,57	3,38	51,50	84,11
	Firefox	W	33,27	5,99	14,25	2,95	0,40	1,04	41,00	7,64
		L	56,70	1,84	11,91	2,88	0,19	0,63	37,50	40,94
	Média		61,87	14,11	24,50	5,32	1,27	1,91	48,88	63,09
95	Chrome	W	33,27	2,09	7,95	3,74	0,08	0,31	54,00	2,75
		A	60,60	0,65	14,02	6,32	0,17	0,56	42,00	5,41
	Firefox	W	24,74	4,78	10,27	2,57	0,17	0,40	45,50	7,09
		L	52,02	1,52	7,67	3,96	0,16	0,39	35,00	181,51
	Média		42,66	2,26	9,98	4,15	0,15	0,42	44,13	49,19

96	Chrome	W	76,71	5,60	34,31	5,89	0,46	2,13	66,00	309,52
		A	71,87	0,72	4,96	6,63	0,17	0,44	40,00	30,86
	Firefox	W	82,60	0,14	10,18	6,40	0,22	1,00	42,50	126,89
		L	68,81	0,82	5,21	17,11	0,17	0,45	38,00	13,62
	Média		75,00	1,82	13,67	9,01	0,26	1,01	46,63	120,22
97	Chrome	W	45,00	13,40	20,32	4,05	1,19	1,55	62,50	6,15
		A	64,50	44,22	50,75	6,16	3,44	4,19	61,00	3,90
	Firefox	W	41,88	7,16	13,28	3,14	1,15	1,77	48,00	7,44
		L	47,34	14,54	21,07	3,21	1,29	1,64	52,00	14,18
	Média		49,68	19,83	26,36	4,14	1,77	2,29	55,88	7,92
98	Chrome	W	71,9	3,6	10,8	13,5	0,1	0,5	53,00	3,15
		A	64,11	1,45	12,28	5,37	0,14	0,39	41,50	50,62
	Firefox	W	70,30	6,81	15,95	7,94	0,94	1,50	46,50	29,89
		L	56,70	2,52	11,45	19,60	0,16	0,56	44,00	57,87
	Média		65,75	3,61	12,62	11,60	0,35	0,74	46,25	35,38
99	Chrome	W	32,10	1,27	5,09	2,33	0,15	0,33	50,5	1,86
		A	37,59	3,22	7,08	2,81	0,17	0,36	42,00	6,22
	Firefox	W	34,46	1,27	8,54	2,37	0,14	0,39	50,00	5,12
		L	59,43	1,11	6,97	2,77	0,16	0,30	37,50	17,22
	Média		40,90	1,72	6,92	2,57	0,16	0,35	45,00	7,60
100	Chrome	W	32,48	0,00	5,00	0,88	0,17	0,31	48,0	1,99
		A	68,79	48,12	59,77	6,72	3,18	4,64	72,50	13,44
	Firefox	W	32,54	0,00	3,05	3,57	0,09	0,35	42,00	6,22
		L	53,97	1,63	7,70	1,92	0,17	0,31	34,50	10,94
	Média		46,95	12,44	18,88	3,27	0,90	1,40	49,25	8,15

Legenda: N.º – Número correspondente ao site da amostra do Apêndice A; **W –** Windows; **A –** Android; **L –** Linux; **Média –** Valor médio dos registos dos quatro testes;
n.d. – Valor não disponível, por não ter sido possível aceder ao site.

Tabela n.º 10 – Agregado de resultados positivos obtidos para os testes aos 100 sites da amostra.

N.º	*Browser*	SO	$\%CPU_{máx}$	$\%CPU_{mín}$	$\%CPU_{m}$	$\%GPU_{máx}$	$\%GPU_{mín}$	$\%GPU_{m}$	Tf_c	v_m
1	Chrome	W	100,00	35,64	**45,83**	13,38	1,47	2,29	**69,50**	81,92
		A	100,00	9,94	**62,25**	8,64	0,97	4,59	**74,00**	658,54
	Firefox	W	59,43	10,24	**23,04**	2,52	0,68	1,30	**69,00**	5,32
		L	65,32	9,09	**20,38**	7,97	1,04	1,70	**56,50**	34,80
2	Chrome	W	64,11	0,08	9,71	5,84	0,17	0,84	**55,00**	5980,16
	Firefox	W	28,27	1,27	5,64	1,63	0,16	0,40	**52,00**	5,75
3	Chrome	W	49,29	24,71	**26,62**	1,03	0,06	0,16	**61,50**	3,41
5	Chrome	W	85,61	0,00	13,14	11,23	0,06	0,67	**53,50**	21,51
10	Chrome	W	70,35	24,25	**27,01**	1,08	0,13	0,25	**59,50**	8,17
	Firefox	W	51,00	2,01	5,54	1,42	0,25	0,40	**50,00**	1,73
12	Chrome	W	83,77	0,14	**25,43**	1,48	0,12	0,25	**65,50**	8,28
	Firefox	W	73,08	0,93	**28,24**	4,30	0,24	0,52	**66,50**	12,64
13	Chrome	W	53,58	24,32	**26,79**	0,55	0,10	0,22	**58,50**	4,26
14	Chrome	W	57,09	2,86	10,89	13,52	0,15	0,59	**55,00**	6,12
	Firefox	W	72,30	0,14	6,98	6,97	0,24	0,58	**53,50**	15,53
18	Chrome	A	97,64	23,96	**36,28**	7,33	2,86	3,86	**62,00**	6,89
	Firefox	W	33,36	12,23	19,21	9,65	1,01	1,44	**55,50**	15,18
19	Firefox	W	39,93	4,82	13,08	6,89	0,25	0,60	**51,50**	153,57
21	Chrome	W	62,95	1,70	10,96	6,16	0,14	0,43	**50,00**	8,51
22	Chrome	W	78,16	0,14	12,83	3,24	0,13	0,64	**60,50**	232,28
	Firefox	L	59,02	1,99	**25,29**	2,68	0,16	1,06	**60,00**	116,37
27	Chrome	W	72,30	0,00	14,12	6,78	0,20	0,81	**54,00**	12,90
		A	64,12	0,00	11,59	10,66	0,10	1,33	**57,50**	1,28
29	Chrome	A	78,55	0,48	**22,56**	14,11	0,14	0,59	**59,50**	17,97
30	Chrome	W	62,52	0,14	12,57	5,04	0,08	0,65	**59,00**	3,59
	Firefox	W	24,68	1,70	8,83	11,07	0,26	1,40	**52,00**	6,30
31	Firefox	W	49,66	0,00	14,24	1,41	0,17	0,48	**50,50**	475,99
33	Chrome	W	6,55	0,00	**34,07**	1,20	0,07	0,31	40,00	3,62
36	Chrome	W	54,47	0,49	7,91	3,41	0,16	0,67	**51,50**	61,11
	Firefox	W	36,05	0,00	2,05	1,42	0,17	0,62	**51,00**	4,50
		L	95,71	1,19	14,07	2,50	0,17	0,62	**50,50**	288,69
40	Firefox	L	45,39	1,13	12,65	9,33	0,16	0,33	**50,50**	119,72
42	Chrome	W	64,11	0,08	17,11	11,18	0,09	0,40	**57,50**	11,20
44	Chrome	W	69,18	5,74	**47,32**	7,08	0,08	1,05	**72,00**	159,38
		A	79,33	49,67	**55,39**	17,27	0,13	1,44	**68,00**	361,44
	Firefox	W	75,46	49,72	**55,03**	4,82	0,13	0,75	**67,50**	139,76
		L	71,55	50,07	**55,11**	3,12	0,14	0,86	**66,00**	45,56
45	Chrome	W	92,59	50,17	**56,88**	7,28	0,13	0,87	**73,00**	28,97
	Firefox	W	64,50	50,12	**55,62**	2,44	0,15	0,96	**69,50**	4,30

48	Chrome	A	55,56	0,00	7,09	6,53	0,17	0,81	**59,00**	1,42
49	Chrome	W	16,99	2,15	**28,61**	6,61	0,15	0,70	**49,00**	86,93
		A	77,38	3,26	**29,70**	22,62	0,62	1,57	**63,00**	43,87
	Firefox	W	71,13	1,70	**23,92**	2,55	0,14	0,42	47,50	59,38
		L	68,80	2,95	**25,51**	4,38	0,13	0,45	**54,50**	74,96
50	Chrome	W	75,47	1,32	**34,29**	5,60	0,14	0,76	**67,50**	267,92
		A	68,79	19,64	**43,31**	7,77	0,14	0,84	**60,00**	201,27
	Firefox	W	61,38	27,05	**41,09**	1,81	0,13	0,47	**61,00**	148,38
		L	64,89	25,96	**43,07**	3,15	0,13	0,79	**62,50**	197,05
52	Firefox	L	66,06	3,17	**31,03**	3,03	0,24	1,46	**60,50**	110,12
53	Chrome	W	77,77	42,27	**52,77**	5,92	0,12	0,83	**71,00**	220,28
		A	68,76	0,00	**37,05**	7,39	0,06	0,89	**73,50**	98,87
	Firefox	W	95,35	41,88	**49,60**	4,80	0,14	0,53	**69,00**	169,27
		L	73,94	42,27	**52,20**	9,56	0,13	0,88	**69,00**	218,06
54	Chrome	W	55,14	45,10	**48,57**	1,56	0,12	0,27	**71,00**	6,65
		A	54,87	46,11	**48,70**	0,75	0,14	0,23	**71,50**	2,40
	Firefox	W	65,67	46,17	**48,76**	6,21	0,13	0,35	**71,50**	3,22
		L	59,04	41,93	**49,05**	2,11	0,14	0,25	**68,00**	7,61
56	Chrome	W	93,34	50,07	**56,22**	21,14	0,13	0,48	**70,00**	88,41
		A	58,26	49,72	**51,66**	1,98	0,12	0,28	**71,00**	2,68
	Firefox	W	59,82	50,07	**51,47**	2,15	0,13	0,27	**71,00**	5,74
		L	75,84	50,07	**51,87**	2,75	0,18	0,26	**71,00**	1158,56
57	Firefox	A	54,45	1,35	**20,44**	4,46	0,06	0,34	**79,50**	5,23
		W	68,01	0,48	**46,04**	1,93	0,14	0,31	**50,00**	4,59
		L	67,98	49,33	**51,84**	10,36	0,08	0,28	**68,50**	15,11
60	Chrome	W	67,61	31,40	**41,07**	2,09	0,22	0,46	**70,50**	19,42
		A	66,06	3,99	**33,20**	5,29	0,39	1,12	**65,50**	27,11
	Firefox	W	67,62	29,00	**41,78**	1,51	0,15	0,48	**69,00**	210,27
		L	76,60	13,40	**42,65**	14,55	0,15	0,63	**64,00**	110,26
61	Firefox	W	53,24	0,47	**31,52**	0,82	0,14	0,37	**59,00**	9,67
62	Firefox	L	59,43	30,95	**35,40**	2,13	1,24	1,40	**65,00**	166,10
64	Chrome	W	52,02	0,00	11,70	5,18	0,07	0,84	**53,50**	28,59
65	Chrome	L	47,73	29,00	**34,39**	2,21	1,24	1,40	47,50	20,38
66	Chrome	A	61,38	0,82	**24,44**	6,43	0,19	2,46	39,00	3,82
	Firefox	L	48,12	1,68	**33,63**	1,96	0,18	1,36	46,00	9,58
67	Chrome	A	63,72	17,82	**38,38**	6,89	2,71	3,89	**59,50**	2,97
	Firefox	L	46,95	30,26	**37,27**	3,48	1,24	1,90	**68,00**	16,34
68	Chrome	A	81,67	27,05	**62,83**	7,35	0,33	5,80	**69,00**	3,47
	Firefox	L	46,95	31,34	**38,49**	9,01	1,20	1,51	**63,50**	10,99
70	Chrome	W	49,27	1,30	15,92	2,79	0,15	0,58	**51,50**	18,07
	Firefox	L	63,76	5,99	14,60	18,64	0,16	0,65	**53,00**	40,81

72	Chrome	W	59,04	2,81	19,27	3,77	0,16	0,95	**53,50**	83,43
		A	92,92	14,71	**54,34**	6,72	0,17	4,40	**50,00**	87,05
	Firefox	L	57,48	34,47	**40,97**	3,54	1,26	1,81	**65,50**	83,39
74	Chrome	W	59,04	0,20	10,47	1,77	0,18	0,52	**56,50**	8,82
		A	50,83	14,49	**26,30**	4,97	2,49	3,06	**58,50**	4,17
	Firefox	W	59,43	1,31	**29,90**	1,88	0,23	0,74	45,00	6,94
77	Chrome	W	50,41	22,35	**30,87**	13,44	2,17	2,83	**62,50**	19,93
		A	72,69	46,56	**63,23**	8,64	3,84	5,51	**69,50**	38,18
	Firefox	W	44,09	8,29	15,39	4,13	1,87	2,34	**50,50**	30,27
		L	58,00	17,69	**32,59**	10,28	1,63	2,46	**65,00**	89,96
82	Chrome	W	80,11	2,48	**24,24**	14,95	0,15	1,72	47,50	409,60
	Firefox	W	31,36	17,30	**24,20**	3,59	1,57	1,88	49,50	15,17
83	Chrome	W	89,52	2,12	**29,87**	15,27	0,04	1,54	45,50	655,36
84	Chrome	W	92,92	42,32	**57,10**	17,90	3,36	4,04	**72,00**	19,77
		A	80,89	61,77	**67,56**	8,16	4,44	5,95	**71,50**	6,66
	Firefox	W	61,77	30,69	**22,02**	10,32	2,09	2,74	**53,50**	19,86
		L	80,13	52,02	**64,40**	8,52	1,81	3,28	**75,00**	83,24
85	Chrome	W	86,74	26,66	**43,62**	18,01	1,47	2,09	**65,50**	48,97
		A	96,15	51,29	**66,63**	14,81	4,31	6,10	**70,50**	221,43
87	Chrome	A	74,25	61,77	**66,78**	6,50	5,44	5,95	**71,50**	11,57
	Firefox	L	57,87	29,00	**40,20**	3,59	1,23	1,79	**66,50**	5,66
89	Chrome	W	65,67	31,28	**38,55**	6,38	2,31	2,82	**60,50**	3,42
90	Chrome	W	71,91	23,62	**30,79**	5,33	2,06	2,64	**67,50**	25,34
92	Chrome	W	74,40	4,01	**20,43**	13,45	0,14	0,95	**56,00**	120,07
		A	63,37	7,94	**36,24**	5,31	0,15	0,49	45,50	67,98
	Firefox	W	54,74	0,48	8,98	4,87	0,15	0,69	**50,00**	62,92
93	Chrome	W	79,44	21,59	**31,43**	5,38	1,57	2,19	**61,50**	127,99
94	Chrome	W	73,48	25,88	**33,46**	7,20	1,91	2,59	**65,50**	119,65
		A	84,01	22,73	**38,38**	8,25	2,57	3,38	**51,50**	84,11
95	Chrome	W	33,27	2,09	7,95	3,74	0,08	0,31	**54,00**	2,75
96	Chrome	W	76,71	5,60	**34,31**	5,89	0,46	2,13	**66,00**	309,52
97	Chrome	W	45,00	13,40	**20,32**	4,05	1,19	1,55	**62,50**	6,15
		A	64,50	44,22	**50,75**	6,16	3,44	4,19	**61,00**	3,90
	Firefox	L	47,34	14,54	**21,07**	3,21	1,29	1,64	**52,00**	14,18
98	Chrome	W	71,90	3,60	10,80	13,50	0,10	0,50	**53,00**	3,15
99	Chrome	W	32,10	1,27	5,09	2,33	0,15	0,33	**50,50**	1,86
	Firefox	W	34,43	1,27	8,54	2,37	0,14	0,39	**50,00**	5,12
100	Chrome	A	68,79	48,12	**59,77**	6,72	3,18	4,64	**72,50**	13,44

Legenda: "Negrito" – Valor preponderante para a classificação de positivo;
N.º - Número correspondente ao site da amostra do Apêndice A; **W –** Windows; **A –** Android;
L – Linux; ▢ **–** Resultado indiciado para *cryptojacking*; ■ **–** Resultado comprovado para *cryptojacking*.

Tabela n.º 11 – Relação entre plataformas de identificação de *cryptojacking* e resultados positivos.

N.º	Site	Notmining	Wappalyzer	Aviso
1	http://moonbit.co.in		X	
2	http://seriesdanko.to		X	
3	https://flaru.com			
5	http://publishyourarticles.net		X	
10	http://www.bayimg.com		X	
12	http://themelike.net		X	
13	http://pixroute.com			
14	http://zeenews.india.com			
18	https://108clip.com		X	
19	http://www.wikioz.ir	?	X	
21	http://ooo-radiocom.ru	X		
22	http://legendaoficial.net		X	
27	http://cherry-market.ru	X		
29	http://medicinarf.ru			
30	https://cryptogears2018.myshopify.com			
31	http://bitblitz.org			
33	http://web.crictime.com			
36	http://gtpl.net	?	X	
40	http://center-pmpk.ru	X	X	
42	http://fanserials.irish			
44	http://mamanema.com			
45	http://paintballgames62.com			
48	http://littlebyte.net			
49	http://biser.info	X		
50	https://tkg.af	X	X	
52	http://funnymama.com			
53	http://madacademy.it	X	X	
54	http://ventureplaza.net	X	X	
56	http://uandblog.com			
57	http://mp3song-s.com			
60	https://www.eonsmoke.com			
61	http://www.gailzavala.com	X		
62	http://360eye.cc	X		
64	http://lqrsw.com	X		
65	http://def18.com	X		
66	http://colleencollection.com.au	X		
67	http://double-sim.com	X		
68	http://312752.top	X		

70	http://atril.com			
72	http://beuyels.com	X		
74	http://wightlo.com	X		
77	http://1365kk.com	X		
82	https://songspk.mobi	X	X	X
83	http://ciberpeliculashd.net	X	X	X
84	https://coinmarketcal.com			
85	https://crisanimex.com	X	X	X
87	https://canalpelis.com	X		
89	https://csubakka.hu	X	X	X
90	http://alinafaucet.win	?	X	
92	https://arabbit.net			
93	http://claimulike.win	X	X	
94	https://sonyoutube.com	X	X	X
95	http://pelisfull.tv	X	X	X
96	http://episode24.pl			
97	http://gametracker.rs			
98	http://nemkacsa.com	X		
99	http://socks24.org	X	X	X
100	http://fans.bz	X	X	

Legenda: ? – Apenas contém um alerta; ☐ **–** Resultado indiciado para *cryptojacking*; ■ **–** Resultado comprovado para *cryptojacking*.