Speech

Federico Zappone

2020-12-09 Wed

Contents

1 Presentazione **2**

2 Monete digitali **2**
2.1 Blockchain 2
2.2 Bitcoin 3
2.2.1 Aumento di valore 3
2.2.2 Oro del XXI Secolo 3
2.2.3 Definito oro perché estraibile 3

3 Mining **3**
3.1 Come funziona? 3
3.2 Compenso 3
3.3 GPU e CPU 3

4 Criptovalute per attacchi informatici **4**
4.1 Criptovalute bene o male? 4
4.2 Ransomware 4
4.3 Anonimato 4
4.4 Criptominers e Cryptojacking 4
4.5 Diffusione 4

5 Perché nel Web? **4**

6 TODO Related Works **4**

7 OpenGL **4**
7.1 WebGL 5

8 Come funziona Hi-Jacket? 5
8.1 Idea . . . 5
8.2 Javascript . . . 5
8.3 GPU.js . . . 5
8.3.1 GPU.js benchmark . . . 5
8.4 XSS . . . 5
8.4.1 Tipi di XSS . . . 5
8.4.2 XSStrike, Traxss e XSSer . . . 5
8.5 Injection automatica . . . 5
8.6 Come testare? . . . 5
8.6.1 Clonare i siti vulnerabili . . . 5
8.6.2 Macchina virtuale . . . 6

9 Difesa 6
9.1 Estensione browser . . . 6
9.2 Code obfuscation . . . 6
9.3 Monitoring . . . 6

10 Deliverables 6
10.1 GitHub . . . 6
10.2 Cryptominer e injector . . . 6
10.3 Possibile difesa . . . 6

1 Presentazione

2 Monete digitali

Chi mi conosce non si stupirà vedendo che si parla di Blockchain

2.1 Blockchain

È una tecnologia basata sul concetto di database distribuito, ovvero un sistema che utilizza un registro condiviso per salvare informazioni, esso è accessibile solo ai nodi della stessa rete ed è rappresentabile come una successione di blocchi contenenti le informazioni

2.2 Bitcoin

2.2.1 Aumento di valore

Da 8 millesimi di dollaro statunitense a 0.50 -> 625 Da 0.50 dollari a 20.000 -> 40.000

2.2.2 Oro del XXI Secolo

2.2.3 Definito oro perché estraibile

3 Mining

3.1 Come funziona?

Consiste nel creare monete virtuali attraverso la risoluzione di alcune funzioni crittografiche necessarie per la validazione delle transazioni e dei blocchi che compongono una blockchain.

3.2 Compenso

Questa operazione termina con un compenso da parte della blockchain al miner, il quale, avendo offerto la sua potenza di calcolo viene premiato con la stessa criptovaluta minata

3.3 GPU e CPU

ASIC, acronimo di Application Specific Integrated Circuit

4 Criptovalute per attacchi informatici

4.1 Criptovalute bene o male?

4.2 Ransomware

4.3 Anonimato

4.4 Criptominers e Cryptojacking

4.5 Diffusione

5 Perché nel Web?

6 TODO Related Works

Ci si è mossi principalmente vero la CPU Sia Musch et al. [6] che Saad et al. [7] mostrano la diffusione di cryptominers basati su CPU nei siti web, inoltre analizzano l'efficacia di tecniche difensive di blacklisting che risultano però essere una protezione insufficiente e poco pratica. Wang et al. [8] forniscono in seguito un metodo di analisi di firme basate su istruzioni della CPU durante l'esecuzione dei moduli WebAssembly. Konoth et al. [9] introducono invece MineSweeper basato anch'esso sul precedente principio di firme ma aggiunge inoltre il rilevamento di eccessive chiamate di sistema di natura crittografica durante l'esecuzione di un programma. Un differente approccio viene fornito da Tahir et al. [10] che presentano MineGuard, un sistema che tramite l'analisi delle prestazioni hardware rileva l'esecuzione di alcuni algoritmi di mining. MineGuard monitora costantemente sia CPU che GPU ed inoltre offre un'ottima soluzione sia in termini di efficienza che di utilizzo di risorse per la sua esecuzione. Belkin, Gelernter e Cidon [11] offrono infine una soluzione dedicata esclusivamente a cryptominers di GPU che risulta essere più pratica in ambito web rispetto alle altre, questo analizzando le pagine web che utilizzano WebGL

7 OpenGL

È una specifica considerata ormai lo standard per quanto riguarda la grafica tridimensionale nei sistemi operativi Unix-like. In particolare OpenGL è stata pensata per architetture parallelizzabili come le GPU e definisce delle API per applicazioni che operano in ambienti 3D

7.1 WebGL

8 Come funziona Hi-Jacket?

8.1 Idea

8.2 Javascript

8.3 GPU.js

8.3.1 GPU.js benchmark

8.4 XSS

8.4.1 Tipi di XSS

- XSS reflected: il payload viene eseguito solo nel momento dell'iniezione;
- XSS stored: il payload viene salvato all'interno della struttura dell'applicativo ed eseguito

ad ogni accesso del contenuto;

- XSS dom-based: il codice sorgente e la risposta del server non vengono modificate, il payload

viene eseguito a runtime senza inoltrare richieste al server ma utilizzando il codice già presente nella pagina.

8.4.2 XSStrike, Traxss e XSSer

8.5 Injection automatica

8.6 Come testare?

8.6.1 Clonare i siti vulnerabili

1. XSSed

8.6.2 Macchina virtuale

9 Difesa

9.1 Estensione browser

9.2 Code obfuscation

9.3 Monitoring

10 Deliverables

10.1 GitHub

10.2 Cryptominer e injector

10.3 Possibile difesa