Attacco e difesa di Cryptojacking basato su GPU

Anna Lisa Ferrara
Dep. of Biosciences and Territory
University of Molise
annalisa.ferrara@unimol.it

Federico Zappone
Dep. of Biosciences and Territory
University of Molise
f.zappone1@studenti.unimol.it

***Sommario*—In quest'ultimo decennio si è molto discusso di monete digitali e delle così dette criptovalute in seguito all'avvento delle blockchain. Il 3 gennaio 2009 veniva scritto il primo blocco di *Bitcoin*dal valore complessivo inferiore a un dollaro statunitense, in seguito raggiunse il suo massimo storico di quasi $20.000 ovvero circa 40.000 volte in più. Divenuto un caso più unico che raro, *Bitcoin* si è posto da apripista a più di 5000 altre criptovalute fino ad essere definito come l'oro del XXI secolo, questo grazie anche al processo di creazione delle criptovalute detto *mining*, come nel caso di pietre e metalli preziosi. Grazie alla privacy che queste criptovalute sono in grado di offrire si sono sviluppati diversi tipi di attacchi informatici tra cui il *cryptojacking* in grado di utilizzare potenza computazionale del computer vittima al fine di effettuare *mining* di criptovalute. In questo articolo sarà mostrato in modo concettuale come sarebbe possibile effettuare un attacco di *criptojacking* in combinazione con il *Cross Site Scripting (XSS)* sfruttando inoltre la potenza computazionale della *Graphics processing unit (GPU)* della vittima.**

***Index Terms*—Cryptojacking GPU XSS Injection**

I. Introduzione

In quest'ultimo decennio si è molto discusso di monete digitali e delle così dette criptovalute in seguito all'avvento delle blockchain. Quest'ultima è una tecnologia basata sul concetto di database distribuito, ovvero un sistema che utilizza un registro condiviso per salvare informazioni, esso è modificabile solo dai nodi della stessa rete ed è rappresentabile come una successione di blocchi contenenti delle informazioni. Contemporaneamente alle blockchain è nata anche la prima criptovaluta, più precisamente, il 3 gennaio 2009 veniva scritto il primo blocco di *Bitcoin* [15] dal valore complessivo inferiore a un dollaro statunitense [11]. In seguito il 6 novembre 2010 il valore di *Bitcoin* era di $0,50, in meno di due anni il prezzo era aumentato di circa 625 volte, e, il 14 aprile 2021, raggiunge il suo massimo storico di circa $64.800 [3] [26] [4]. Divenuto un caso più unico che raro, *Bitcoin* si è posto da apripista a più di 5000 altre criptovalute [5] fino ad essere definito come l'oro del XXI secolo. Questa definizione non è dovuta solo all'incredibile aumento del prezzo negli ultimi anni ma anche ad una delle caratteristiche chiave che sia l'oro che la maggior parte delle criptovalute condivide, il processo di "estrazione" definito appunto come *mining* nel campo delle monete digitali. Il *mining* di criptovalute 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. Questa operazione termina con un compenso da parte della blockchain al *miner*, il quale, avendo offerto la sua potenza di calcolo viene premiato con un compenso monetario. Tali calcoli sono in generale eseguiti da sistemi informatici dedicati a questo specifico processo, essi sono divisi in due macro gruppi in base all'hardware che utilizzano: quelli che sfruttano la Central Processing Unit (CPU) e quelli che sfruttano la Graphics processing unit (GPU). I primi prendono il nome di *ASIC*, acronimo di *Application Specific Integrated Circuit*, ovvero circuiti costruiti per la risoluzione di un calcolo ben specifico che risultano però molto inefficienti su altri tipi di algoritmi. I sistemi basati su GPU sono invece spesso molto più prestanti, le schede video riescono infatti a effettuare più calcoli al secondo rispetto alle CPU che risultano quindi meno redditizie nella maggior parte dei casi di *mining*. D'altro canto per le GPU risulta essere molto più difficile la gestione delle temperature e inoltre comportano costi maggiori sia in termini di assemblaggio che di costi energetici per il mantenimento. Questi ultimi aspetti hanno un notevole impatto per quanto riguarda il *mining*: il costo di acquisto delle componenti è nettamente aumentato negli ultimi anni, sia a causa dell'avanzamento delle tecnologiche più efficienti, sia a causa della grande domanda da parte degli interessati al *mining*.

Con l'aumentare dei costi, e allo stesso tempo delle opportunità di guadagno offerte dal mondo in crescita delle blockchain, le criptovalute hanno iniziato a risaltare agli occhi del crimine informatico. Più precisamente la tecnologia blockchain, e di conseguenza una buona parte delle criptovalute, posseggono una caratteristica molto importante per i cyber criminali, ovvero garantiscono una certa forma di anonimato. Le criptovalute infatti sono difficilmente riconducibili ad una persona fisica diversamente da un conto bancario classico. Le criptovalute sono infatti collegare ad un portafoglio digitale, detto appunto *wallet*. L'accesso ai *wallets* non è però regolamentato, e quindi non collegato fisicamente a qualcuno. Questa caratteristica ha portato a un enorme utilizzo delle criptovalute per lo svolgimento di azioni illecite, nel 2017 infatti si è riscontrato un netto aumento dei così detti *ransomware* [22], ovvero virus che una volta bloccato il sistema sul quale sono eseguiti chiedono un riscatto per il suo sblocco. Tale pagamento di tale riscatto è richiesto sotto forma di criptovalute per mantenere l'anonimato. Successivamente si è arrivati a una forma di attacco più "intelligente" e meno invasiva, ovvero i *cryptominers*. Definito appunto come "l'anno dei cryptominers", il 2018 vede la stessa impennata di casi di *ransomware*

dell'anno precedente sotto una nuova forma di attacco che consiste nell'utilizzare potenza computazionale della vittima per generare criptovalute 1. Il tutto avviene seguendo un basso profilo, tramite programmi infetti che vengono installati sul computer o, come più recentemente si è affermato, attraverso script malevoli presenti all'interno di pagine web comuni. La differenza tra l'utilizzo di programmi eseguibili e gli script presenti online sta principalmente nella loro rintracciabilità e facilità di utilizzo, infatti quelli che operano attraverso il web sono più difficili da individuare e analizzare rispetto a programmi che devono necessariamente essere installati dall'utente e che, quindi, sono sotto l'occhio diretto di antivirus e delle politiche dettate dal sistema operativo.

L'utilizzo della GPU in all'interno di browser è ad oggi possibile, anche se non largamente diffuso, tramite l'utilizzo di alcune librerie e specifiche web. *OpenGL* (*Open Graphics Library*) è considerata ormai lo standard per quanto riguarda la grafica tridimensionale in sistemi operativi *Unix-like*, in particolare, essa è stata pensata per architetture parallelizzabili come le GPU e definisce delle *API* per applicazioni che operano in ambienti 3D. Su questo standard sono basate altre librerie che permettono l'utilizzo della GPU in ambito web come *WebGL*. Quest'ultima è una *Web-based Graphics Library* ovvero una libreria pensata per la gestione di elementi grafici all'interno del web, essa fornisce delle *API* per grafica 3D in un contesto *HTML5* tramite l'utilizzo del *Document Object Model (DOM)*. Da *WebGL* si arriva poi a *GPU.js*, ovvero una libreria implementata interamente attraverso il linguaggio *JavaScript* e pensata per sfruttare l'accelerazione hardware delle GPU attraverso l'utilizzo del medesimo linguaggio.

L'utilizzo di un linguaggio di scripting web come *Javascript* è rilevate, in quanto esso può essere utilizzato per portare a termine attacchi che sfruttano vulnerabilità di tipo *Cross Site Scripting (XSS)*. Gli attacchi di tipo *XSS* sono tra i più diffusi all'interno del web, infatti, secondo il report di Positive Technologies Security [17], la percentuale di questi attacchi è salita dall'occupare il 77,9% nel 2017 all'88,5% di tutte le tipologie di attacchi web registrate nel 2018. Secondo Precise Security [18] invece, in rapporto a tutti i tipi di attacchi sferrati verso le grandi compagnie di Europa e Nord America nel 2019, la percentuale di attacchi di *Cross Site Scripting* risulta essere del 39%, superando più del doppio la percentuale degli attacchi di *SQL Injection*.

L'*XSS* consiste nell'introdurre del codice arbitrario lato client all'interno dei siti web con il fine di eseguire una serie di attacchi rivolti ai visitatori. Questa vulnerabilità affligge i siti dinamici che non effettuano un controllo sugli input lato client, il che porta ad una "fusione" tra il payload, ovvero il codice inserito dall'attaccante, e il codice reale della pagina. Questa tipologia di attacchi si suddivide a sua volta in tre gruppi:

- 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.

Il resto dell'articolo è strutturato nel modo seguente: Sezione II introduce quello che è lo stato dell'arte, .

II. Stato dell'arte

Le GPU grazie alla loro potenza offrono quindi nella maggior parte dei casi dei ricavi maggiori nel *mining* rispetto alle CPU, di contro però non sono facilmente utilizzabili in ambito web. Ciò ha portato infatti ad uno sviluppo maggiore dei *cryptominers* basati su CPU e, di conseguenza, a sistemi di difesa che si concentrano su di essi. Musch et al. [14] e Saad, Khormali e Mohaisen [20] mostrano la diffusione dei *cryptominers* basati su CPU all'interno del web, inoltre analizzano l'efficacia di tecniche difensive di blacklisting che risultano però essere una protezione non sempre efficiente sebbene pratica. Wang et al. [25] mostra in seguito un metodo di analisi di firme basate su istruzioni della CPU durante l'esecuzione dei moduli *WebAssembly*. Konoth et al. [12] introduce invece *MineSweeper* basato anch'esso sul principio di firme ma con l'aggiunta del rilevamento di eccessive chiamate di sistema di natura crittografica legate agli algoritmi di mining durante l'esecuzione di un programma. Kharraz et al. [11] dimostra invece che come l'analisi della CPU generi una grande quantità di falsi positivi all'interno della navigazione web. Un differente approccio viene fornito da Tahir et al. [23] che presenta *MineGuard*, un sistema che tramite l'analisi delle prestazioni hardware rileva l'esecuzione di alcuni algoritmi di *mining*. *MineGuard* monitora costantemente l'hardware del computer e inoltre offre un'ottima soluzione sia in termini di efficienza che di utilizzo di risorse per la sua esecuzione. Belkin, Gelernter e Cidon [1] offre infine una soluzione dedicata esclusivamente a *cryptominers* di GPU che risulta essere decisamente più pratica in ambito web rispetto alle altre, andando a limitare le pagine web che utilizzano *WebGL* [10].

III. Risultati

IV. Sviluppi futuri

Riferimenti bibliografici

[1] Alex Belkin, Nethanel Gelernter e Israel Cidon. "The Risks of WebGL: Analysis, Evaluation and Detection". In: *European Symposium on Research in Computer Security*. Springer. 2019, pp. 545–564.

[2] Prithvi Bisht e VN Venkatakrishnan. "XSS-GUARD: precise dynamic prevention of cross-site scripting attacks". In: *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*. Springer. 2008, pp. 23–43.

[3] *Bitcoin Wiki*. https://en.bitcoinwiki.org/wiki/Bitcoin_history.

[4] CoinGecko. *All Time High list*. https://www.coingecko.com/it/monete/ath.

[5] *Coinlore all Coins*. https://www.coinlore.com/all_coins.

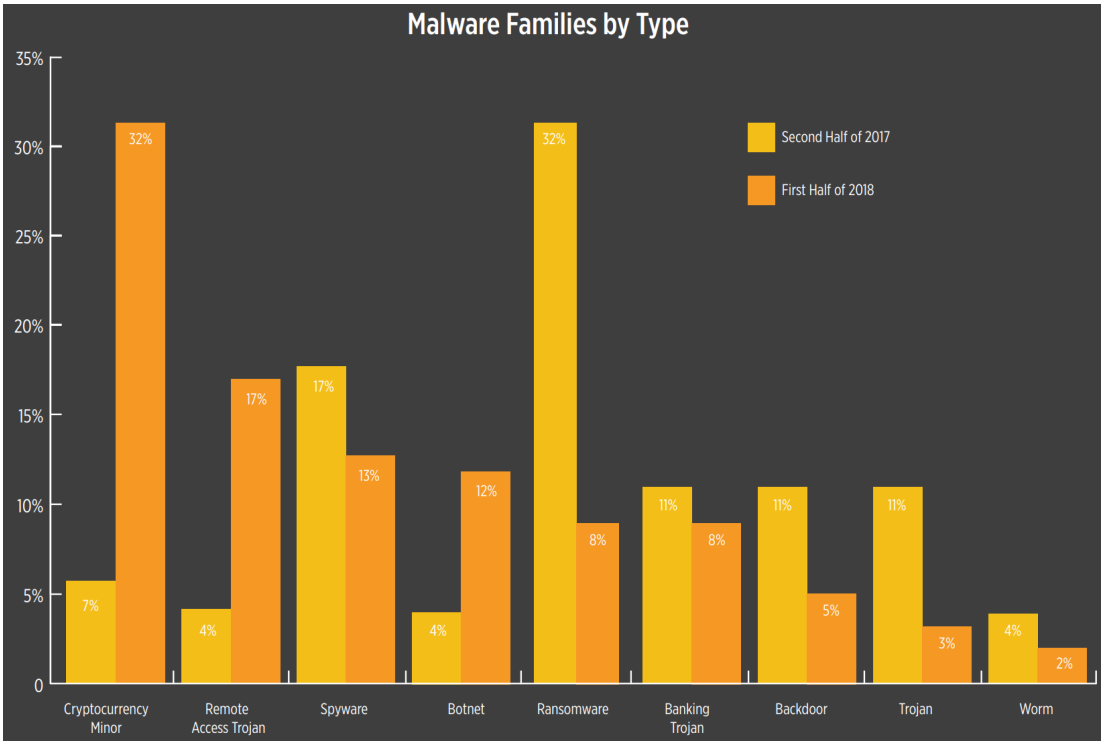

Figura 1. Top Malware Families by type, 2018, *Skybox Vulnerability Report Trends* [22]

[6] GPU.js community. *GPU.js benchmark*. https://gpu.rocks/#/benchmark.

[7] epsylon. *XSSer*. https://github.com/epsylon/xsser.

[8] gpujs. *GPU.js*. https://github.com/gpujs/gpu.js.

[9] The Khronos Group Inc. *OpenGL*. https://www.opengl.org/.

[10] The Khronos Group Inc. *WebGL*. https://github.com/KhronosGroup/WebGL.

[11] Amin Kharraz et al. "Outguard: Detecting in-browser covert cryptocurrency mining in the wild". In: *The World Wide Web Conference*. 2019, pp. 840–852.

[12] Radhesh Krishnan Konoth et al. "Minesweeper: An in-depth look into drive-by cryptocurrency mining and its defense". In: *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*. 2018, pp. 1714–1730.

[13] M4cs. *Traxss*. https://github.com/M4cs/traxss.

[14] Marius Musch et al. "Web-based Cryptojacking in the Wild". In: *arXiv preprint arXiv:1808.09474* (2018).

[15] Satoshi Nakamoto. *Bitcoin: A peer-to-peer electronic cash system*. Rapp. tecn. Manubot, 2019.

[16] OWASP. *Cross Site Scripting (XSS)*. https://owasp.org/www-community/attacks/xss/.

[17] Positive Technologies Security. *Penetration testing of corporate information systems: statistics and findings, 2019*. https://www.ptsecurity.com/ww-en/analytics/corp-vulnerabilities-2019/.

[18] Precise Security. *Cross-Site Scripting (XSS) Makes Nearly 40% of All Cyber Attacks in 2019*. https://www.precisesecurity.com/articles/cross-site-scripting-xss-makes-nearly-40-of-all-cyber-attacks-in-2019/.

[19] s0md3v. *XSStrike*. https://github.com/s0md3v/XSStrike.

[20] Muhammad Saad, Aminollah Khormali e Aziz Mohaisen. "End-to-end analysis of in-browser cryptojacking". In: *arXiv preprint arXiv:1809.02152* (2018).

[21] Monirul I Sharif et al. "Impeding Malware Analysis Using Conditional Code Obfuscation." In: *NDSS*. 2008.

[22] *Skybox Vulnerability Report Trends*. https://lp.skyboxsecurity.com/rs/440-MPQ-510/images/Skybox_Report_Vulnerability_Threat_Trends_2018_Mid-Year_Update.pdf.

[23] Rashid Tahir et al. "Mining on someone else's dime: Mitigating covert mining operations in clouds and enterprises". In: *International Symposium on Research in Attacks, Intrusions, and Defenses*. Springer. 2017, pp. 287–310.

[24] W3Techs. *Usage statistics of JavaScript as client-side programming language on websites*. https://w3techs.com/technologies/details/cp-javascript.

[25] Wenhao Wang et al. "Seismic: Secure in-lined script monitors for interrupting cryptojacks". In: *European Symposium on Research in Computer Security*. Springer. 2018, pp. 122–142.

[26] *Wired - Trasformazione di Bitcoin*. https://www.wired.it/economia/finanza/2019/01/03/bitcoin-2009-trasformazione-storia/.

[27] xssed. *xssed*. http://www.xssed.com/pagerank.