Relazione di Crittografia

Cryptojacking: quando il tuo Computer lavora per qaualcun altro.

Elvis Perlika

0000970373

Corso di Crittografia
A.A. 2023-2024
Prof. Luciano Margara

Indice

1 Introduzione

1.1 Definizione

Il Cryptojacking, in Italiano "Dirottamento di risorse", è una forma di attacco informatico che sfrutta la potenza di calcolo di un utente, senza che esso ne sia consapevole, per minare criptovalute. [1]

Gli Hacker hanno come obbiettivo quello di prendere il controllo del maggior numero possibile di sistemi con l'obbiettivo di minare quante più criptovalute, illecitamente. Questo sistema di hacking non punta unicamente la classica utenza di Personal Computer ma cerca di sfruttare anche le risorse di Server e infrastrutture Cloud e in generale ogni tipologia di sistema computazione con un accesso alla rete Internet.

La caratteristica fondamentale di questo malware è far sì che la vittima sia ignara dei processi in background, che si occupano di minare, e permettergli di usare la propria macchina normalmente. Ovviamente, il tutto, a discapito di un sovraccarico della macchina e conseguente surriscaldamento, presenza di lag, maggior consumo elettrico (che nel caso di servizi Server o Cloud porta ad avere fatture particolarmente elevate) e riduzione delle performance generali.

Questo paper si propone di analizzare il fenomeno del cryptojacking, i metodi di attacco, le tecnologie coinvolte e i relativi aspetti tecnici per poi esporre le contromisure per prevenire e individuare questi malware al intero delle proprie macchine. In particolare, nella sezione "Aspetti Tecnici" si andarà ad analizzare nel dettaglio il mining di Monero, una delle criptovalute più utilizzate per il cryptojacking e l'algoritmo CryptoNight, utilizzato per minare Monero.

1.2 Storia

Una delle prime forme di cryptojacking è stata scoperta nel Giugno 2011, quando l'azienda Symantec Corporation iniziò a sospettare che le botnet [1] potessero minare Bitcoin segretamente, sebbene la GPU di una sola macchina impiegherebbe molto tempo per minare una transizione in criptovalute, utilizzando una grande quantità di macchine si riesce a suddividere il lavoro e ridurre il tempo.

Una serie di attacchi rilevanti di cryptojacking sono stati scoperti dal 2011 al 2021. L'ultimo è relativo al "2021 Microsoft Exchange Server data breach" [3], tale brec-

[1] Una botnet è un gruppo di dispositivi connessi a Internet , ognuno dei quali esegue uno o più bot . Le botnet possono essere utilizzate per eseguire attacchi DDoS (distributed denial-of-service), rubare dati, [1] inviare spam e consentire all'aggressore di accedere al dispositivo e alla sua connessione. Il proprietario può controllare la botnet utilizzando un software di comando e controllo (C&C). [2] La parola "botnet" è una parola risultata dalla unione delle parole " robot " e " network ". Il termine è solitamente utilizzato con una connotazione negativa o malevola.[2]

cia, creata nel Gennaio 2021 ha permesso numerosi attacchi tra qui diversi di tipo cryptojacking.

Il cryptojacking è emerso come una minaccia significativa nel campo della cybersecurity intorno al 2017, con l'introduzione di Coinhive, dismesso poi a Marzo 2019 era un servizio di mining di criptovalute attraverso i browser web, che andava a utilizzare parte o tutta la potenza di calcolo per minare criptovalute Monero (approfondimento nella sezione "Aspetti Tecnici").

1.3 Struttura del documento

Fornisci una panoramica della struttura del documento, indicando brevemente cosa verrà trattato nelle diverse sezioni.

1.4 Importanza

Spiega perché l'argomento è rilevante o significativo. Questo aiuta a contestualizzare la tua discussione e a motivare l'interesse del lettore.

1.5 Problema e Motivazione

Identifica il problema specifico che il tuo documento cerca di risolvere e spiega perché è importante affrontarlo.

2 Come funziona

Il mining, cioè il processo che Bitcoin e altre cripto valute utilizzano per coniare virtualmente nuove monete digitali e certificare le transazioni, usando le relative monete, è completamente lecito.

Nel dettaglio troviamo vaste reti decentralizzate di computer in tutto il mondo che verificano e proteggono le blockchain, ovvero i registri virtuali che documentano le transazioni di criptovalute. In cambio del contributo della loro potenza di elaborazione, l'utente del computer della rete che per primo risolve i calcoli complessi dovuti alla certificazione della transizione viene premiato con nuove monete. Si tratta di un circolo virtuoso: i minatori mantengono e tutelano la blockchain, la blockchain assegna le monete, le monete fungono da incentivo ai minatori per continuare a mantenere la blockchain. Il mining è l'unico modo per rilasciare nuove cripto monete nella rete ed è un processo che richiede molta potenza di calcolo con un effort inversamente proporzionale al mining effettuato portando così ad un aumento della difficoltà di mining e ad una conseguente crescita dei costi.

Il cryptojacking sfrutta questo processo, ma in modo illecito. Gli hacker inseriscono codice malevolo nei siti web o nei messaggi di posta elettronica che infettano i computer delle vittime e li trasformano in macchine per il mining riducendo i costi e aumentando i guadagni.

3 Metodi di attacco

I metodi per attaccare un sistema con il cryptojacking sono molteplici e variano a seconda del tipo di sistema che si vuole attaccare. I metodi più comuni sono:

3.1 Attaccare direttamente i Personal Computer

Attaccare uno o più PC è il classico metodo per creare un sistema di cryptojacking. Tipicamente l'hacker riesce ad iniettare il suo software di mining all'interno della macchina usando tecniche come:

- **Fileless malware**: possono essere di 2 tipologie:
  - *Fully Fileless Malware*: non esegue nessun file sul disco ma tutte le attività possono essere osservate in memoria. Gli hacker possono anche, attraverso la rete, inivare pacchetti malevoli che installano backdoor che risiedono nella memoria kernel.
  - *Fileless Malware with Indirect File Activity*: non scrive direttamente i file sul disco, ma gli autori delle minacce possono installare un comando PowerShell all'interno del repository WMI configurando un filtro WMI per la persistenza. Anche se in teoria l'oggetto WMI dannoso esiste su un disco, non tocca il file system sul disco. Si tratta quindi di un attacco senza file poiché, secondo Microsoft [34], "l'oggetto WMI è un contenitore di dati multiuso che non può essere rilevato e rimosso".[5]
- **Schemi di phishing**: è il modo più semplice con cui gli aggressori di cryptojacking possono rubare risorse è inviare agli utenti un'e-mail dall'aspetto legittimo che li incoraggi a fare clic su un collegamento che esegue il codice per inserire uno script di cryptomining sul proprio computer. Funziona in background e invia i risultati tramite un'infrastruttura di comando e controllo (C2[2]).
- **Embedded di script malevoli al interno di siti o web app**: gli hacker possono sfruttare script all'interno dei siti, che eseguiti automaticamente dai browser, minano le cripto valute. Questo metodo è molto più diffuso e meno invasivo rispetto al precedente, poiché non sscarica alcun codice nel dispositivo.

3.2 Cercare server e dispositivi di rete vulnerabili

I server sono un obbiettivo molto ambito per gli hacker, in quanto sono dispositivi molto potenti e spesso connessi a Internet 24/7. Gli hacker possono sfruttare vulnerabilità come

[2]Command and Control Infrastructure: anche conosciuto come C&C o C2 è il set di strumenti e tecniche che un un hacker utilizza per mantenere la commuicazione con il computer precedentemente compresso.

Log4J[3] per iniettare i propri sistemi di cryptojacking in queste potenti macchine. Spesso i server compromessi vengono anche utilizzi come potente per accedere con maggior semplicità ad altri dispositivi per eseguire attacchi più complessi ed orizzontali.

3.3 Attaccare il sistema di produzione di software

Un altro metodo molto comune è quello di attaccare il sistema di seminare repository open-souce nelle quali è stato iniettato il loro codice malevolo. Grazie ai programmatori che utilizzano questi codici è possibile per gli hacker raggiungere un numero elevato di macchine e scalare velocemente il loro sistema di mining. Una volta entrati nella macchina del programmatore, possono cercare di accedere anche ai server, ai dispositivi di rete oppure ai servizi cloud ai quali esso è connesso. In alternativa possono puntare a sub-iniettare questi script all'interno dei progetti che i programmatori stanno sviluppando.

3.4 Fare leva sulle infrastrutture cloud

Come per i server, anche le infrastrutture cloud sono un obbiettivo molto ambito poiché permettono di effettuare computazioni ancora più veloci. Uno dei metodi più comuni per farlo è scansionare le API dei container esposti e utilizzare tale accesso per avviare il caricamento del software di mining sulle istanze dei container o sui server cloud interessati. L'attacco è in genere automatizzato con un software di scansione che cerca server accessibili alla rete Internet pubblica con API esposte o che permettono l'accesso senza autenticazione. Come per i server, gli aggressori sfruttano il cloud service violato ed attraverso lo stesso puntano a raggiungere altre infrastrutture simili. Questi sono gli attacchi più redditizi.
L'aspetto rilevante, in tutti gli approcci sopra citati, è che gli hacker possano accedere a quante più macchine computazionali.

[3] "La vulnerabilità Log4j, conosciuta anche come Log4Shell, è una vulnerabilità critica scoperta nella libreria di registrazione Apache Log4j nel novembre del 2021. Sostanzialmente, Log4Shell concede agli hacker il controllo totale dei dispositivi eseguendo versioni di Log4j senza patch." - IBM

4 Aspetti tecnici di Monero

Non è obbiettivo di questo paper approfondire il tema delle criptovalute in senso generale ma si vuole trattare il tema del mining in modo più specifico. Nella seguente sezione si andrà ad analizzare il mining di Monero, una delle criptovalute più utilizzate per il cryptojacking.

La criptovaluta Monero, inizialmente nota come BitMonero, è stata creata nell'aprile 2014 come deriva della valuta proof-of-concept CryptoNote. Monero significa "denaro" nella lingua esperanto.

CryptoNote è una criptovaluta ideata da vari individui. Un white paper di riferimento che lo descrive è stato pubblicato sotto lo pseudonimo di Nicolas van Saberhagen nell'ottobre 2013. Grazie a CryptoNote e al suo algoritmo di hashing, CryptoNight, Monero è diventata una delle criptovalute più popolari per il mining.

Una delle filosofie di Monero è quella di mantenere un mining egualitario, in modo che tutti possano avere la possibilità di fare mining. Per raggiungere questo obiettivo, utilizza un algoritmo particolare ideato e sviluppato dai membri della community della criptovaluta: RandomX . Questo algoritmo PoW è resistente agli ASIC, il che rende impossibile costruire hardware specializzato per fare mining di Monero. I miner sono obbligati ad utilizzare hardware di livello consumer e competere lealmente.

4.1 Fondamentali

Le curve ellittiche sono la funzione matematica che sta alla base della crittografia delle criptovalute. Queste curve sono utilizzate per creare le chiavi pubbliche e private che permettono di firmare e verificare le transizioni. Procediamo con criterio per capire come funzionano le curve ellittiche, questo sarà fondamentale per comprendere il funzionamento di Monero e delle sue caratteristiche di privacy.

4.1.1 Aritmetica Modulare

L'aritmetica modulare, detta anche *Aritmetica dell'orologio*, è un sistema di aritmetica degli interi, in cui i numeri "si avvolgono su loro stessi" ogni volta che raggiungono i multipli di un determinato numero n, detto **modulo**.

Inconsciamente utilizziamo l'aritmetica modulare ogni volta che guardiamo un orologio. Ad esempio, se sono le 10:00 e aggiungo 3 ore, il risultato sarà 1:00 e non 13:00. Questo perché l'orologio è un sistema di 12 ore, quindi il modulo è 12; questo è il motivo per cui viene chiamata *aritmetica dell'orologio*.

Diciamo che per calcoalre $c = a \mod b$ possiamo immaginare un asse di numeri interi e posizionarci si a e 'saltare' con passi di lunghezza b fino a raggiungere un valore intero che sia ≥ 0 e $< b$, questo sarà il nostro c. Ad esempio:

$$-5 \mod 3 = 1 \qquad \text{oppure} \qquad 4 \mod 3 = 1$$

Formalmente possiamo definire l'equazione $c = a \mod b$ come $a = bx + c$ dove x è il quoziente e c è il resto di $a \mod b$.

Ne seguono alcune proprietà che verranno definite in seguito.

4.1.2 Curve Ellittiche

Definiamo una curva ellittica E su un campo finito F_p dove p è un numero primo a 256 bit e la presentiamo in forma di Weierstrass come:

$$E : y^2 = x^3 + ax + b \mid x, y \in F_p$$

in cui a e b sono i parametri della curva che ne defiscono la forma e la posizione. Le coordinate (x, y) sulla curva ellittica che possono prendere qualsiasi valore all'interno di F_p formano un Gruppo Abeliano [4]. Questo particolare gruppo ci permette, scegliamo 2 punti P e Q sulla curva che useremo per risolvere R andando a eseguire l'operazione di somma $P + Q = R$ con R che sarà un altro punto sulla curva.

Prendiamo gli scalari p, q valori interi random di grandezza n tali che $p, q \in o, 1^n$.

Il Standards for Efficient Cryptography (SEC) è un set di curve ellittiche proposte per l'uso nel campo della crittografia. Una delle più note e utilizzate è la **Secp256k1** definita dalla equazione

$$y^2 = x^3 + 7 \mod p$$

dove

$$p = 2^{256} - 2^{32} \underbrace{-2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1}_{-977}$$

.

Questa curva è la base per la crittografia di Bitcoin e altre criptovalute. Questa funzione possiede diverse qualità tali che è stata applicata, non solo nel abito delle criptovalute, ma anche in altri campi per rendere le commuicazione sicure; come quello del IoT. Monero, invece, utilizza la curva Ed25519, di cui parleremo più avanti.

4.2 Scambio di chiavi Diffie-Hellman con curve ellittiche

Il protocollo di scambio di chiavi Diffie-Hellman (DH), inventato nel 1976, nato dalla collaborazione dei ricercatori Whitfield Diffie e Martin Hellman, è il primo protocollo a permettere a 2 parti di communicare attraverso un canale insicuro senza necessità di condiversi una chiave segreta previa commuicazione. Vennero così introdotti i cifrari a chaive pubblica. Matematicamente, il protocollo DH si basa sul problema della fattorizzazione e sul problema del logaritmo discreto nell'algebra modulare.

[4] Un gruppo abeliano è un gruppo in cui l'operazione beneficia della proprietà commutativa È anche detto: Gruppo Commutativo

Definiamo p un numero reale random tale che $0 < k < l$ che chiameremo *private key* e calcoliamo la relativa *public key* $P = k \cdot G$ dove G è il generatore del gruppo abeliano in questione.

Un classico scambio di segreti tra Bob e Alice, utilizzando le curve ellittiche, avviene nel seguente modo:

1. Alice e Bob generano le proprie chiavi pubbliche e private (p_A, S_A) e (p_B, S_B) rispettivamente. Entrambi condividono le proprie chiavi pubbliche ma non quelle private.

2. Assumendo
$$X = p_A \cdot S_B = p_A \cdot p_B \cdot G = p_B \cdot p_A \cdot G = p_A \cdot S_A$$
Alice e Bob dovranno calcolarsi, privatamente: $X = p_A \cdot S_B$ e $X = p_B \cdot S_A$. Queste saranno le chiavi condivise.

   Un osservatore esterno non riuscirà a calcolare S, cioè il segreto, in modo semplice proprio a causa del problema di Diffie-Hellman. Infatti trovare S a partire da S_A e S_B è un problema computazionalmente estremamente difficile.

4.3 Shnorr Signature

In crittografia, per Shnorr Signature si intende l'algoritmo di firma digitale ideato da Clauss Schnorr nel 1989. È uno dei primi protocolli basati sulla **impraticibiltà** nel risolvere il problema del logaritmo discreto, la sua funzione è permette di dimostrare ad una delle 2 parti in comunicazione di conoscere la chiave privata relativa a quella pubblica senza rivelare, appunto, quella privata. Questo algoritmo ci sarà utile per quando tratteremo le Ring Signature (tradotte: Firme ad Anello).

Algoritmo

È fondamentale che tutti gli utenti della commuicazione concordino sul gruppo abeliano G, di ordine q, generato da g e per assunzione in questo gruppo il problema del logaritmo discreto sia molto difficile. Oltre al gruppo devono conconrdare anche su una funzione di hash sicura $H : \{0,1\}^* \to \mathbb{Z}/q\mathbb{Z}$.

Generazione delle chiavi Si sceglie una chiave privata $p \in \mathbb{Z}_q$ e si calcola la chiave pubblica $S = g^{-p}$.

Firma Per firmare un messaggio m si procede nel seguente modo:

1. si genera un numero reale random $k \in \mathbb{Z}_q$

2. si calcola $x = g^k$ con $x \in G$

3. si calcola $r = H(x||m)$ dove $||$ rappresenta la concatenazione in stinghe di bit

4. si calcola $c = k + p \cdot r$ con $e \in \mathbb{Z}_q$

Abbiamo, così, creato la firma (c, r) per il messaggio m. Chiameremo c la 'challenge' e r la 'response'.

Verifica Per verificare la firma (c, r) si procede nel seguente modo:

1. si calcola $x_v = g^c \cdot y^r$

2. si calcola $r_v = H(x_v||m)$

Se $r_v = r$ allora la firma è valida.

Dimostrazione

$$x_v = g^c \cdot y^r = g^{k+p \cdot r} \cdot g^{-p \cdot r} = g^k = x$$

ed in seguito:

$$r_v = H(x_v||m) = H(x||m) = r$$

quindi il messaggio firmato corrisponde a quello verificato.

Anche se un intruso, senza conoscere la chiave privata, avesse creato la firma (c, r) sarebbe stato trascurabile, quindi un verificatore può essere sicuro che il messaggio non sia stato manomesso.

4.4 Curva Ellittica Ed25519

Ed25519 è una particolare *Twisted Edwards elliptic curve* che utilizza Monero per le operazioni crittografiche. La curva è definita dal campo $F_{2^{255}-19}$ e dalla curva ellittica:

$$-x^2 + y^2 = 1 - \frac{121665}{121666} x^2 y^2$$

La communità scientifica (il NIST) pensa che questa curva non sia così sicura e affidabile.

Le curve Twisted Edwards sono di ordine $N = 2^c l$ con l numero primo e c un intero positivo. Nel caso di Ed25519 il suo ordine è di 76 cifre e quindi l è a 253 bits.

$l = 2^3 \cdot 7237005577332262213973186563042994240857116359379907606001950938285454250989$

Il campo $F_{2^{255}-19}$ è codificato in 32 byte, ovvero 256 bit. Di conseguenza, qualsiasi punto in Ed25519 potrebbe essere espresso utilizzando 64 byte poichè includono sia una

rappresentazione del punto R che un valore scalare S derivato da una computazione su una funzione di hash H:

$$S = (H + \textit{private key} \times H) \mod l$$

Applicando le tecniche di point compression, descritte di seguito, tuttavia, è possibile ridurre questa quantità della metà, a 32 byte utilizzando tecniche di "Point Compression" [5].

4.5 Shnorr Signature Avanzato

In Shnorr base utilizziamo una sola chiave ma possiamo rendere Shnorr più sofisticato utilizzando più chiavi. Questo è il caso dello schema Multi Layer Linkable Spontaneous Anonymous (MLSAG), uno schema di firma che permette a più utenti di firmare un messaggio in modo anonimo.

È spesso vantaggioso dimostrare che la stessa chiave privata è stata utilizzata per generare chiavi pubbliche su basi diverse. Per esempio, consideriamo una chiave pubblica standard kG e un segreto condiviso di Diffie-Hellman kR con la chiave pubblica di un'altra persona, dove le basi sono rispettivamente G e R. In questo contesto, possiamo dimostrare la conoscenza del logaritmo discreto k relativo a kG, provare la conoscenza di k in kR, e confermare che k è identico in entrambe le situazioni, senza tuttavia rivelare il valore di k.

È possibile trovare una *Non-interactive proof*[6] a pagina 25 del white paper di Monero [8].

Chiamiamo Non-Interactive Proof è un metodo crittografico in cui una parte (il provatore) può dimostrare a un'altra parte (il verificatore) che una certa affermazione è vera senza interagire direttamente con il verificatore durante il processo di prova, diversamente dal tradizionale *Zero-knowledge proofs* che necessità di una interazione tra le parti simultanea.

4.6 Privacy in Monero

Monero può essere estratto sia da CPU che da GPU, ma la prima è molto più efficiente. E' evidente che sia la cripto valuta più pratica per il cryptojacking, poiché può essere

[5] Le tecniche di point compression (compressione dei punti) sono metodi utilizzati in crittografia ellittica per ridurre la quantità di dati necessari per rappresentare un punto su una curva ellittica. Questo è particolarmente utile per ridurre l'uso di memoria e banda, specialmente in applicazioni che richiedono l'invio o la memorizzazione di grandi quantità di punti su curve ellittiche, come nelle firme digitali o nei protocolli di scambio di chiavi.

[6]

minata solo su macchine a livello consumer, le quali sono faccilemente accessibili da cybercriminali attraverso i metodi precedentemente citati. Inoltre, utilizza una blockchain[7] supportata da un **Privacy-enhancing technologies** sofisticato, il quale derivava da CryptoNight. Al fine di fornire privacy e anonimato, Monero, si basa su due concetti importanti: Stealth Address e Ring Signature.

4.6.1 Address

In tutte le blockchain, per ogni utente viene generato un indirizzo, questo è tutto ciò che serve per ricevere pagamenti. Poichè il libro mastro è pubblico, tutti possono vedere gli indirizzi e le transizioni e si può facilmente comprendere per ogni indirizzo l'ammontare di cripto valuta che possiede.

Monero, diveresamente da altre cripto valute come BitCoin, utilizza nella transazione due coppie di chiavi private/pubbliche: (k^v, K^v) e (k^s, K^s). La seconda coppia è l'indirizzo del utente, mentre la prima è la corrispondente chiave privata. Indichiamo con k^v le *view key* e con k^s la *spend key*.

La chiave di visualizzazione viene utilizzata per verificare se un'uscita è associata al proprio indirizzo, mentre la chiave di spesa consente di "spendere" quell'uscita in una transazione per poi confermare che è stata spesa.

Di seguito spiegherò in sintesi alcune scelte di design di Monero per garantire la massima riservatezza e anonimato nelle transizioni. Se si vuole approfondire si può consultare il white paper di Monero [8] nelle pagine 37-42.

One-time address Se, generalmente, un utente deve condividere il proprio indirizzo per ricevere pagamenti, Monero utilizza un sistema di indirizzi monouso. Come facciamo a condividere un indirizzo monouso? Utilizzando uno scambio di tipo Diffie-Hellman, così anche un osservatore che conosce tutti gli address non può comprendere chi stia eseguendo la transizione e verso chi.

Facciamo un esempio: Alice vuole inviare 10 Monero a Bob. Bob ha le proprie coppie di chiavi (k^v_B, K^v_B) e (k^s_B, K^s_B) e Alice conosce le chiavi pubbliche di Bob quindi il suo inidirizzo.

Parafrasando Butrin[8]:

> Sia il destinatario (chiamiamolo "Bob") che il mittente ("Alice") possono generare un indirizzo invisibile per la transazione. Tuttavia, solo il destinatario, Bob, può controllare la transazione. Un altro modo di pensare a un indirizzo

[7] Libro contabile digitale condiviso in rete, è il sistema fondamentale di una criptovaluta in quanto tiene memoria di tutte le transizioni eseguite nella storia della realtiva criptovaluta. Viene detta blockchain poiché è una catena di blocchi, ognuno rappresenta una transizione che viene agganciata alla catena attraverso la risoluzione di calcoli complessi (mining).

[8] Vitalik Buterin, co-fondatore di Etherium

invisibile è come un indirizzo di portafoglio legato crittograficamente all'indirizzo pubblico di Bob, ma che viene rivelato solo alle parti che effettuano la transazione. [6]

Questi One-time address sono anche detti Stealth Address. Il team di Buterin ha progettato un sistema di indirizzi nascosti (anche detto SAP [9]) chiamato BaseSAP. Il protocollo mira a fornire un meccanismo leggero che consenta agli utenti di generare indirizzi temporanei, mantenendo la completa compatibilità con le versioni precedenti e non richiedendo modifiche alla blockchain principale. BaseSAP è basato sul cifrario assimetrico su curve ellittiche Secp256k1, migliorato attraverso l'integrazione di "tags di visualizzazione" utili a rendere più efficiente l'analisi rispetto ai comuni DKSAPs [10].

Questo protocolli sono la base per le implementazioni DKSAP usate in Monero. Da quando DKSAP è nato, ha portato molti ricercatori a studiare e trovare nuovi modi per migliorarlo:

Author	**Year**	**Technique**	**Nr. of Keys**	**Extra Data Requirement**	**BaseSAP Compatible**
Bytecoin [12]	2011	Elliptic Curve Diffie-Hellman key exchange (ECDH)	One	Yes	Yes
Van Saberhagen [1]	2013	ECDH + Dual-Key Stealth Address Protocol (DKSAP)	Two	Yes	Yes
Todd [2]	2014	ECDH	One	Yes	Yes
Monero [3]	2014	ECDH + DKSAP	Two	Yes	Yes
Courtois and Mercer [13]	2017	ECDH + DKSAP with multiple key pairs	Multiple	Yes	Yes
Fan [14]	2018	ECDH + DKSAP with improved parsing	Two	Yes	Yes
Fan *et al.* [7]	2019	Bilinear Mapping	One	No	N/A
Liu *et al.* [8]	2019	Lattice-based SAP	Two	No	N/A
Feng *et al.* [15]	2020	ECDH + DKSAP with improved parsing	Two	No	N/A
Lee and Song [16]	2021	ECDH	One	Yes	Yes
Feng *et al.* [5]	2021	Bilinear Mapping	Two	Yes	Yes
Mohideen and Kumar [17]	2022	ECDH + DKSAP with improved parsing	Two	No	N/A

Figura 1: Sommario dei lavori di ricerca sulle Stealth Address e compatibilità BaseSAP

l

1. Alice genera una reale random $r \in \mathbf{Z}l$ e calcola il One-time address

$$K^o = \mathcal{H}_n(rK_B^v)G + K_B^s$$

e definisce K^o come l'indirizzo di Bob, al quale specifica l'importo di 10 Monero ed il valore rG e pubblica il tutto sulla blockchain.

2. Bob, una volta ricevuti i dati, calcola $k_B^v rG = rK_B^v$ e calcola $K'^s = K^o - \mathcal{H}_n(rK_B^v)G$. Una volta che ha ha compreso se $K'^s = K^s$ comprendo che l'outout è per lui.

[9]Stealth Address Protocol
[10]Dual-Key Stealth Address Protocols

3. una volta che Bob avrà confermato che l'output è per lui utilizzando la sua *view key*, potrà firmare un messaggio con la sua *spend key* e inviarlo alla rete per dimostrare di essere Bob e ricevere i Monero accordati.

Subaddress Un'altra tecnica per garantire la privacy è quella di utilizzare gli *subaddress*. Ogni utente può generare dei subaddress partendo dal proprio address. Questi subaddress possono essere utilizzati per ricevere pagamenti, possiamo immaginare l'address come una 'Banca' e i subaddress come i relativi 'Bancomat'. Oltre ad essere utili per aumentare la privacy, l'utente che crea i propri subaddress può utilizzarli per distinziare una transazione da un'altra.

4.6.2 Amount Hiding

4.6.3 Ring Signature

5 Popolarità

La popolarità è dovuta al potenziale guadagno, guadagno molto facile da crearsi poiché per definizoione il cryptojacking punta a sfruttare risorse in possesso di altri in modo gratuito. Così, anche considerando la volatilità delle cripto valute, esempio principe BitCoin, i margini di guadagno sono abbastanza alti da rendere il crimine un vero e proprio business.

6 Prevenire e individuare

7 Casi reali

7.1 WatchDog targets Docker Engine API endpoints and Redis servers

Un gruppo di hacker, chiamato WatchDog, ha attaccato i server Docker[11] e Redis[12]. Il gruppo riusciva ad infiltrarsi nei Docker Engine API attraverso la porta 2375 aperta, una volta dentro, gli intrusi, potevano accedere alla Shell di comando.

Payload Viene caricato nel container uno script **cronb.sh** che va a controllare lo stato del container ed eventualmente eseguire un secondo script **ar.sh**, il quale va sabatore completamente il container e caricare un miner XMRRig[13]. Un ultimo Payload è una serie di script che gli intrusi usano per puntare ad altri sisteme collegati alla rete del container.[11]

7.2 Alibaba ECS instances in cryptomining crosshairs

Come nel caso di Docker, anche in questo caso gli hacker hanno puntato alle sfrutture cloud, ma di Alibaba. I gruppi in question esembrerebbero essere TeamTNT, Kinsing ed altri.

I server Alibaba ECS[14] sono forniti con un preinstallato agente di sicurezza.

Di seguito un codice specifico del malware che crea regole firewall per eliminare i pacchetti in entrata da intervalli IP appartenenti a zone e regioni interne di Alibaba.

Quando un malware di cryptojacking è attivo su un'istanza Alibaba ECS, l'agente di sicurezza installato, se lo rileva, notifica la presenza di uno script dannoso. A quel punto, è compito dell'utente, gestore della piattaforma, intervenire per arrestare l'infezione e le attività malevole. Alibaba Cloud Security fornisce indicazioni su come procedere, ma la responsabilità principale dell'utente rimane quella di prevenire l'infezione fin dall'inizio.

[11] Docker è una piattaforma software che permette di creare, testare e distribuire applicazioni con la massima rapidità. Docker raccoglie il software in unità standardizzate chiamate container che offrono tutto il necessario per la loro corretta esecuzione, incluse librerie, strumenti di sistema, codice e runtime. - AWS

[12] Redis, un sistema di gestione di database NoSQL lanciato nel 2009, utilizza un modello di archiviazione basato su coppie chiave/valore. Ogni dato è memorizzato in un dizionario, in cui una chiave univoca è associata a un valore specifico, rendendo semplice il recupero delle informazioni.

[13] Un software di mining di Monero

[14] Elastic Compute Service

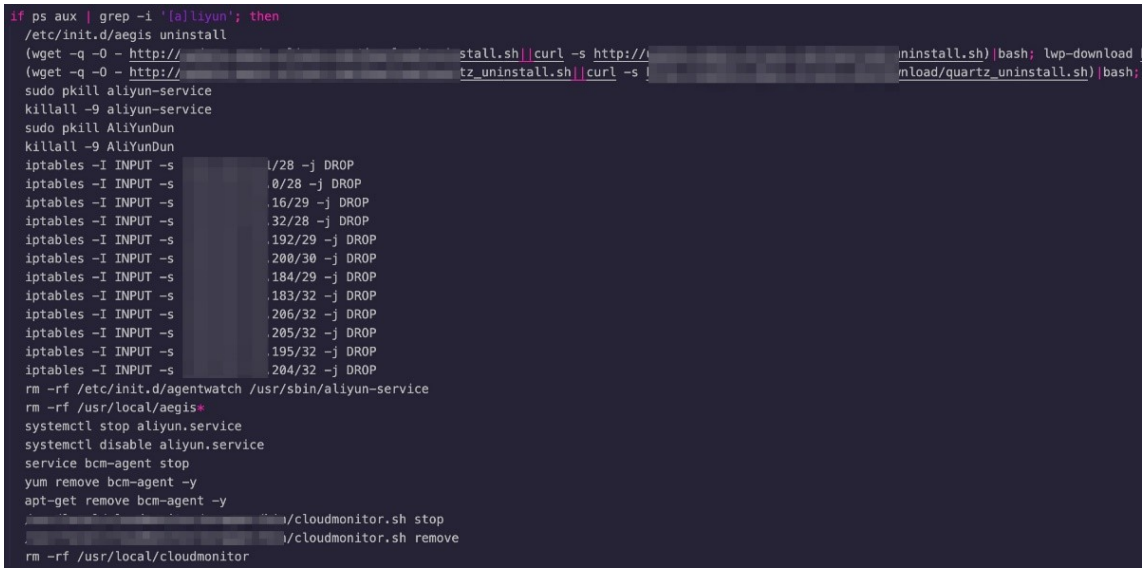

Figura 2: Codice dannoso che modifica le regole del firewall

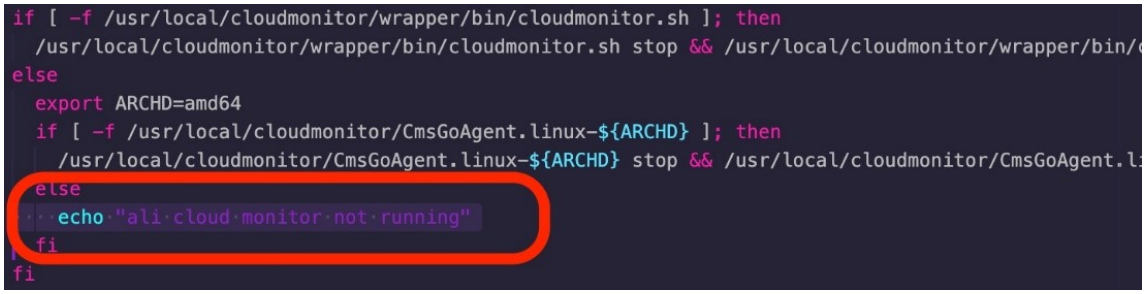

Figura 3: Script che disabilità l'agente di sicurezza di Alibaba

8 Bibliografia

Riferimenti bibliografici

[1] Ericka Chickowski, Cryptojacking explained: How to prevent, detect, and recover from it, CSO, 20 Giugno, 2022

[2] Botnet, Wikipedia

[3] 2021 Microsoft Exchange Server data breach, Wikipedia

[4] Monero, Wikipedia

[5] Fileless malware, IEEE Xplore

[6] Valerio Diaco, *Conosci gli Stealth Address per star lontano dai radar?*, Rypto.it, 15 Lugio 2023

[7] Anton Wahrstatter , Matthew Solomon, Ben DiFrancesco, Vitalik Buterin, and Davor Svetinovic *BaseSAP: Modular Stealth Address Protocol for Programmable Blockchains*, JOURNAL OF LATEX CLASS FILES, VOL. 14, NO. 8, Agosto 2021, pp. 1–6

[8] Koe, Kurt M. Alonso, Sarang Noether, *Zero to Monero: Second Edition - A technical guide to a private digital currency; for beginners, amateurs, and experts* 4 Aprile 2020 (v2.0.0)

[9] Margara Luciano, *Diffie Hellman, Crittografia su Curve Ellittiche* A.A. 2023-2024

[10] Simon Josefsson and Ilari Liusvaara. Edwards-Curve Digital Signature Algorithm (EdDSA). RFC 8032, Gennaio 2017. https://rfc-editor.org/rfc/rfc8032.txt

[11] WatchDog Targets Docker And Redis Servers In New Cryptojacking Campaign, 06 Giugno 20222

[12] David Fiser, Alfredo Oliveira, Groups Target Alibaba ECS Instances for Cryptojacking, 15 Novembre 2021