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 **2**
1.1 Definizione 2
1.2 Storia 2

2 Come funziona **3**

3 Metodi di attacco **3**
3.1 Attaccare diretamente i Personal Computer 3
3.2 Cercare server e dispositivi di rete vulnerabili 4
3.3 Attaccare il sistema di produzione di software 4
3.4 Fare leva sulle infrastrutture cloud 4

4 Aspetti tecnici **5**

5 Popolarità **5**

6 Prevenire **5**

7 Bibliografia **5**

1 Introduzione

1.1 Definizione

Il Cryptojacking 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 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.

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 breccia, 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

[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]

o tutta la potenza di calcolo per minare criptovalute Monero[2] mentre l'utente navigava il sito.

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 diretamente 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

[2]Un particolare tipo di criptovaluta che si presta particolarmente bene al mining utilizzando la CPU e caratterizzato da una blockchain con tecnologie di miglioramento della privacy per offuscare le transazioni per ottenere l'anonimato e la fungibilità.[4]

- Schemi di phishing
- Embedded di script malevoli al interno di siti o web app

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[3]).

In alternativa 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 Log4J[4] 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 subiniettare 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

[3]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.

[4]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.[5]

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.

4 Aspetti tecnici

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 molto alti.

6 Prevenire

7 Bibliografia

Riferimenti bibliografici

[1] Cryptojacking explained, CSO

[2] Botnet, Wikipedia

[3] 2021 Microsoft Exchange Server data breach, Wikipedia

[4] Monero, Wikipedia

[5] Log4J, IBM