TeamTNT, il nuovo worm che batte criptomoneta attraverso il cloud di Amazon

Un nuovo worm di cryptomining, si sta diffondendo attraverso il cloud **AWS** (Amazon Web Services) per ottenere accessi multipli non autorizzati e estrarre criptovaluta **Monero** tramite lo strumento di mining XMRig.

Questo è quanto emerge dalla pubblicazione dei ricercatori di Cado Security secondo cui il worm distribuirebbe anche ulteriori malware e tool di sicurezza offensivi:

- punk.py, uno strumento di post-exploitation SSH;
- log_clean.c, uno strumento di pulizia registro;
- il Rootkit Diamorphine;
- la backdoor Tsunami IRC

Attraverso questo malware i criminal hacker riescono, oltre che prendere di mira specificamente AWS per scopi di cryptojacking, a carpire credenziali locali e eseguire scansioni Internet alla ricerca di piattaforme Docker e Kubernetes pericolosamente esposte in rete.

TeamTNT: analisi del codice malevolo

Il team di Cado Security ha attribuito il worm al gruppo TeamTNT (gruppo altamente prolifico apparso all’inizio dell’anno e di cui precedenti ricerche Trend Micro, Malware Hunter Team e r3dbU7z hanno fornito evidenze), trovando diversi riferimenti all’interno del codice malware.

Tra questi, in particolare, spicca il dominio chiamato teamtnt [.] Red che ospita il payload e che presenta una home page intitolata “TeamTNT RedTeamPentesting” con un elenco indirizzi di diverse sandbox pubbliche.

Come noto AWS CLI (l’interfaccia a riga di comando di AWS link https://docs.aws.amazon.com/cli/latest/userguide/cli-configure-files.html) archivia le credenziali ed ulteriori dettagli di configurazione (per gli account e la stessa infrastruttura AWS) in file non crittografati contenuti rispettivamente nelle sottocartelle / .aws / credentials e / .aws / config presenti nella directory home oppure root del sistema AWS.

Pertanto il codice malevolo procede, utilizzando il comando curl, a scaricare dai sistemi compromessi i suddetti file (.credentials e .config) predefiniti di AWS, archiviandoli sul server criminale, presidiato ed in ascolto all’indirizzo sayhi.bplace [.] Net.

- Lo script malware TeamTNT, che contiene del codice copiato da un altro worm Kinsing osservato in precedenti campagne (è solito per il cryptomining copiare il codice della concorrenza, dicono i ricercatori) e progettato per arrestare gli strumenti di Alibaba Cloud Security, prevede anche delle routine:
- per eseguire la scansione (tramite il port scanner masscan) delle API Docker aperte, per poi successivamente avviare l’installazione del payload;

• per utilizzare il miner XMRig ed estrarre la criptovaluta Monero generando profitti illeciti. A tal proposito i ricercatori hanno scoperto almeno 119 sistemi compromessi e due wallet Monero collegati al gruppo hacker.

Attività di contrasto

Nonostante l’importo sino adesso racimolato ammonti a 3 XMR (circa 300 $) e che queste tipologie di attacchi non siano

particolarmente sofisticate, resta alta la probabilità che il numero dei sistemi compromessi possa aumentare ulteriormente, considerando anche il trend crescente nell'utilizzare ambienti cloud e container da parte delle aziende, aprendo di fatto una nuova superfice di attacco per i criminal hacker. Non sono nemmeno da escludere prossime iniziative fotocopia.

I ricercatori di sicurezza consigliano alle aziende come attività di contrasto:

- di identificare i propri e eventuali sistemi che archiviano i file di credenziali AWS eliminandoli se non necessari;
- utilizzare strumenti firewall per limitare gli accessi alle API Docker;
- monitorare il traffico di rete delle connessioni ai pool di mining e di quelle che inviano credenziali AWS via HTTP;
- di implementare gli IoC pubblicati sugli apparati di sicurezza.

IoC

Monero Wallets
88ZrgnVZ687Wg8ipWyapjCVRWL8yFMRaBDrxtiPSwAQrNz5ZJBRozBSJrCYffurn1Qg7Jn7WpRQSAA3C8aidaeadAn4xi4k
85X7JcgPpwQdZXaK2TKJb8baQAXc3zBsnW7JuY7MLi9VYSamf4bFwa7SEAK9Hgp2P53npV19w1zuaK5bft5m2NN71CmNLoh

Domain Names
6z5yegpuwg2j4len.tor2web[.]su
dockerupdate.anondns[.]net
teamtntisback.anondns[.]net
sayhi.bplaced[.]net
teamtnt[.]red
healthymiami[.]com (Compromised)
rhuancarlos.inforgeneses.inf[.]br (Compromised)

IP Addresses
129.211.98[.]236
85.214.149[.]236
203.195.214[.]104

File-Hashes
3a377e5baf2c7095db1d7577339e4eb847ded2bfec1c176251e8b8b0b76d393f
929c3017e6391b92b2fbce654cf7f8b0d3d222f96b5b20385059b584975a298b
705a22f0266c382c846ee37b8cd544db1ff19980b8a627a4a4f01c1161a71cb0

https://www.key4biz.it/teamtnt-il-nuovo-worm-che-batte-criptomoneta-attraverso-il-cloud-di-amazon/318639/