Scarleteel - Exploit kubernetes & AWS

Historique

Non disponible pour le moment.

Description

An advanced hacking operation dubbed 'SCARLETEEL' targets public-facing web apps running in containers to infiltrate cloud services and steal sensitive data.

SCARLETEEL was discovered by cybersecurity intelligence firm Sysdig while responding to an incident in one of their customers' cloud environments.

While the attackers deployed cryptominers in the compromised cloud environments, the hackers showed advanced expertise in AWS cloud mechanics, which they used to burrow further into the company's cloud infrastructure.

Sysdig believes the cryptojacking attack was used as a decoy for the threat actors' real purpose, which was the theft of proprietary software.

SCARLETEEL attacks

The SCARLETEEL attack began with the hackers exploiting a vulnerable public-facing service in a self-managed Kubernetes cluster hosted on Amazon Web Services (AWS).

Once the attackers access the container, they download an XMRig coinminer, believed to serve as a decoy, and a script to extract account credentials from the Kubernetes pod.

The stolen credentials were then used to perform AWS API calls to gain persistence by stealing further credentials or creating backdoor users and groups in the company's cloud environment. These accounts were then used to spread further through the cloud environment.

Depending on the AWS cluster role configuration, the attackers may also gain access to Lambda information, such as functions, configurations, and access keys.

Commands executed by the attacker

Commands executed by the attacker

Source: Sysdig

Next, the attacker uses the Lambda functions to enumerate and retrieve all proprietary code and software along with its execution keys and the Lambda function environment variables to find IAM user credentials and leverage them for subsequent enumeration rounds and privilege escalation.

S3 bucket enumeration also occurs at that stage, and files stored in cloud buckets are likely to contain valuable data for attackers, such as account credentials.

"During this particular attack, the attacker was able to retrieve and read more than 1 TB of information, including customer scripts, troubleshooting tools, and logging files," reads Sysdig's report

> "The 1 TB of data also included logging files related to Terraform, which was used in the account to deploy part of the infrastructure. These Terraform files will play an important part in the later step where the attacker tried to pivot to another AWS account." - Sysdig.

To minimize the traces left behind, the attacker attempted to disable CloudTrail logs in the compromised AWS account, adversely impacting Sysdig's investigation.

However, it was evident that the attacker retrieved Terraform state files from the S3 buckets containing IAM user access keys and a secret key for a second AWS account. This account was eventually used for lateral movement within the organization's cloud network.

Terraform secrets found by TruffleHog

Terraform secrets found by TruffleHog

Source: Sysdig

Securing your cloud-based infrastructure

As the enterprise increasingly relies on cloud services to host their infrastructure and data, hackers are following along, becoming experts in APIs and management consoles to continue their attacks.

The SCARLETEEL attack proves that a single vulnerable point in an organization's cloud environment could be enough for persistent and knowledgeable threat actors to leverage it for network infiltration and sensitive data theft.

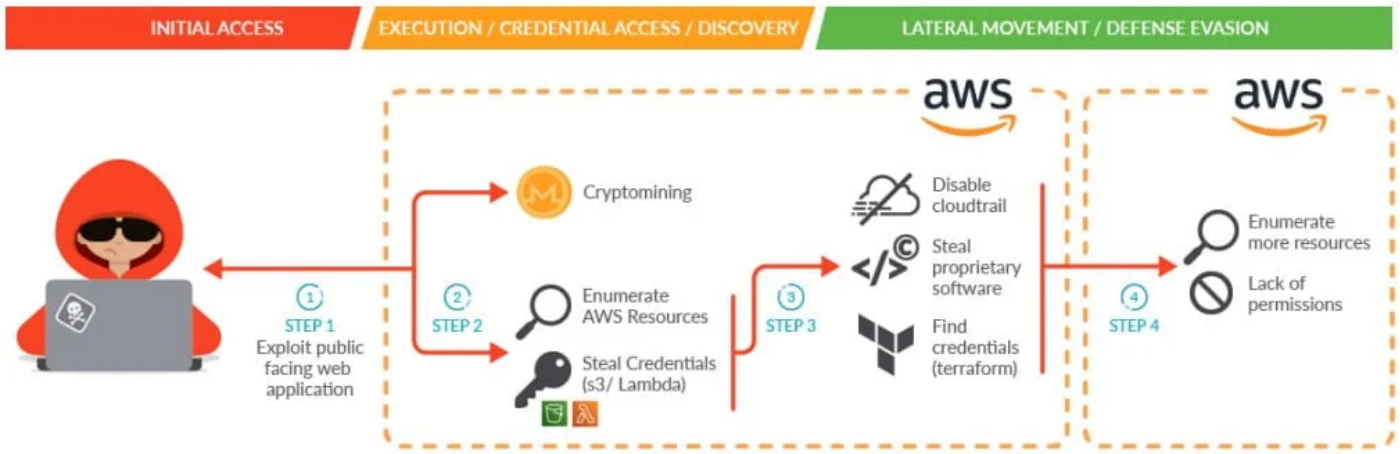
Sysdig suggests that organizations take the following security measures to protect their cloud infrastructure from similar attacks:

- Keep all your software up to date.
- Use IMDS v2 instead of v1, which prevents unauthorized metadata access.
- Adopt principles of least privilege on all user accounts.

- Scope read-only access on resources that may contain sensitive data like Lambda.
- Remove old and unused permissions.
- Use key management services like AWS KMS, GCP KMS, and Azure Key Vault.

Sysdig also recommends implementing a comprehensive detection and alerting system to ensure that malicious activities by attackers are promptly reported, even when they evade protection measures.

Schéma



Sources

https://heimdalsecurity.com/blog/scarleteel-cloud-attack-used-kubernetes-aws-steal-source-code/

https://www.bleepingcomputer.com/news/security/scarleteel-hackers-use-advanced-cloud-skills-to-steal-source-code-data/

Revision #1
Created 2026-07-17 15:09:52 UTC by Olivier
Updated 2026-07-17 15:09:54 UTC by Olivier