Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

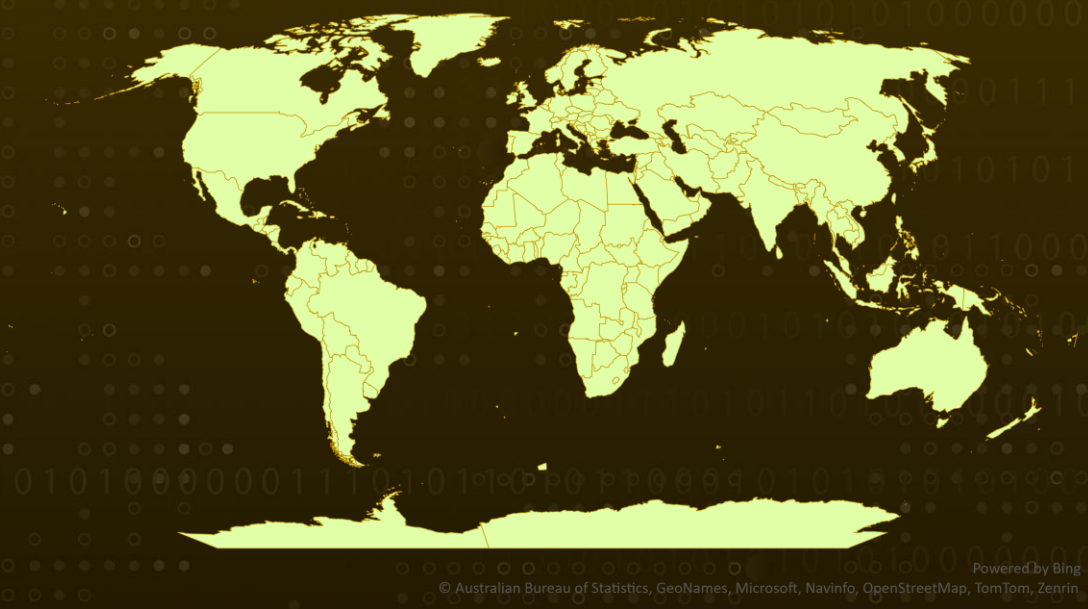
Highly Sophisticated SCARLETEEL Cloud Attack That Stole Proprietary Data

Date of Publication	Admiralty Code	TA Number
March 1, 2023	A1	TA2023110

Summary

Date: February 28, 2023
Attack Region: Worldwide
Attack: The SCARLETEEL attack was a highly sophisticated cloud operation that involved the theft of proprietary data by exploiting a compromised Kubernetes container, escalating privileges into an AWS account, and attempting to pivot to other connected AWS accounts.

Attack Regions



Attack Details

#1

The attack, dubbed SCARLETEEL, involved the theft of proprietary data through a highly sophisticated cloud operation. The attacker gained access through a compromised Kubernetes container and then escalated privileges to an AWS account, stealing both software and credentials. They also attempted to expand their reach throughout the organization using a Terraform state file to pivot to other connected AWS accounts.

#2

This attack was unique in its level of sophistication and knowledge of AWS cloud mechanics, including Elastic Compute Cloud (EC2) roles, Lambda serverless functions, and Terraform. The attacker's initial access was gained by exploiting a public-facing service in a self-managed Kubernetes cluster within the victim's AWS account.

#3

Once inside, the attacker launched a cryptominer and obtained credential access through Instance Metadata Service (IMDS) v1, using cluster role permissions to enumerate AWS resources and find credentials of other IAM users. They then used these credentials to move laterally, disabling CloudTrail logs to evade detection and stealing proprietary software.

Recommendations

Security Leaders

Phishing simulations and routine education and awareness training and communications rarely account for MFA fatigue and web browser hygiene. Integrate and communicate all lessons learned.

Security Engineers

- **Uni5 Users:** This is an actionable threat advisory in HivePro Uni5. Prioritize and block all indicators attributed to the threat actors and attacks through your Command Center. Test your controls with Uni5's Breach & Attack Simulation.
- **All Engineers:** Refer to and action upon the 'Potential MITRE ATT&CK TTPs' & 'Indicators of Compromise (IoC)' on the following pages.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0005 Defense Evasion	TA0006 Credential Access
TA0007 Discovery	TA0008 Lateral Movement	T1190 Exploit Public-Facing Application	T1569 System Services
T1552 Unsecured Credentials	T1552.005 Cloud Instance Metadata API	T1526 Cloud Service Discovery	T1528 Steal Application Access Token
T1082 System Information Discovery	T1574 Hijack Execution Flow	T1562 Impair Defenses	T1567 Exfiltration Over Web Service
T1570 Lateral Tool Transfer			

Indicators of Compromise (IOCs)

TYPE	VALUE
IPV4	80[.]239[.]140[.]66, 45[.]9[.]148[.]221, 45[.]9[.]148[.]121, 45[.]9[.]249[.]58

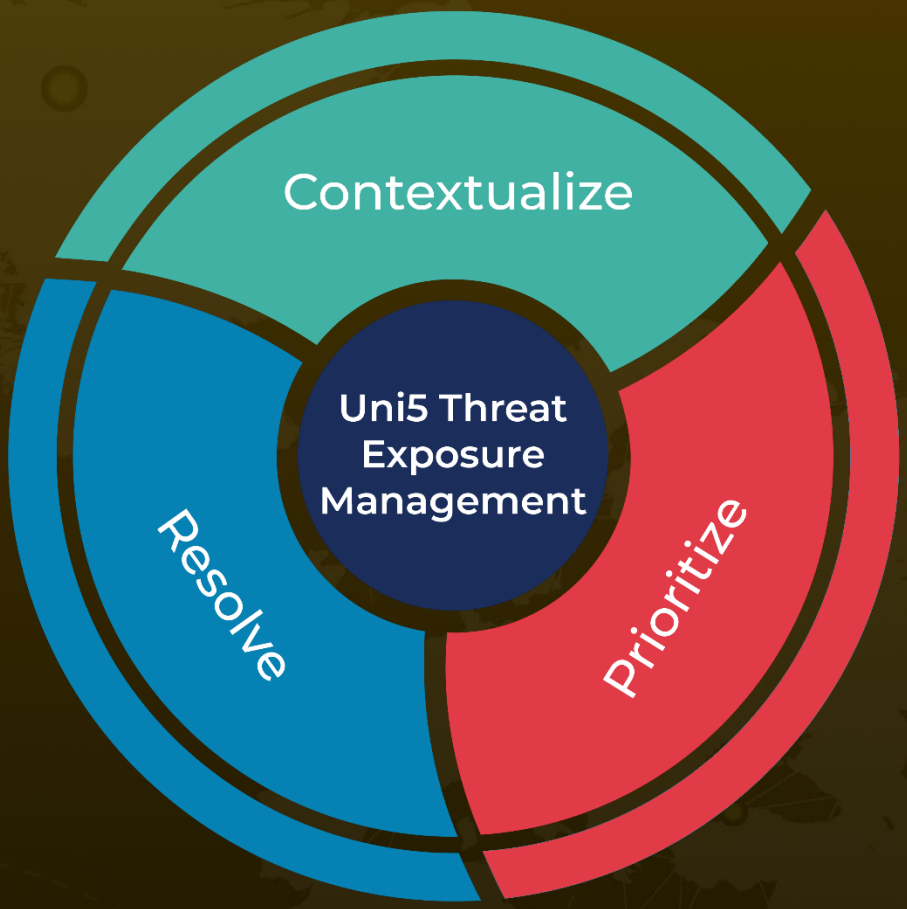
References

https://sysdig.com/blog/cloud-breach-terraform-data-theft/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

March 1, 2023 • 1:20 AM

More at www.hivepro.com