Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

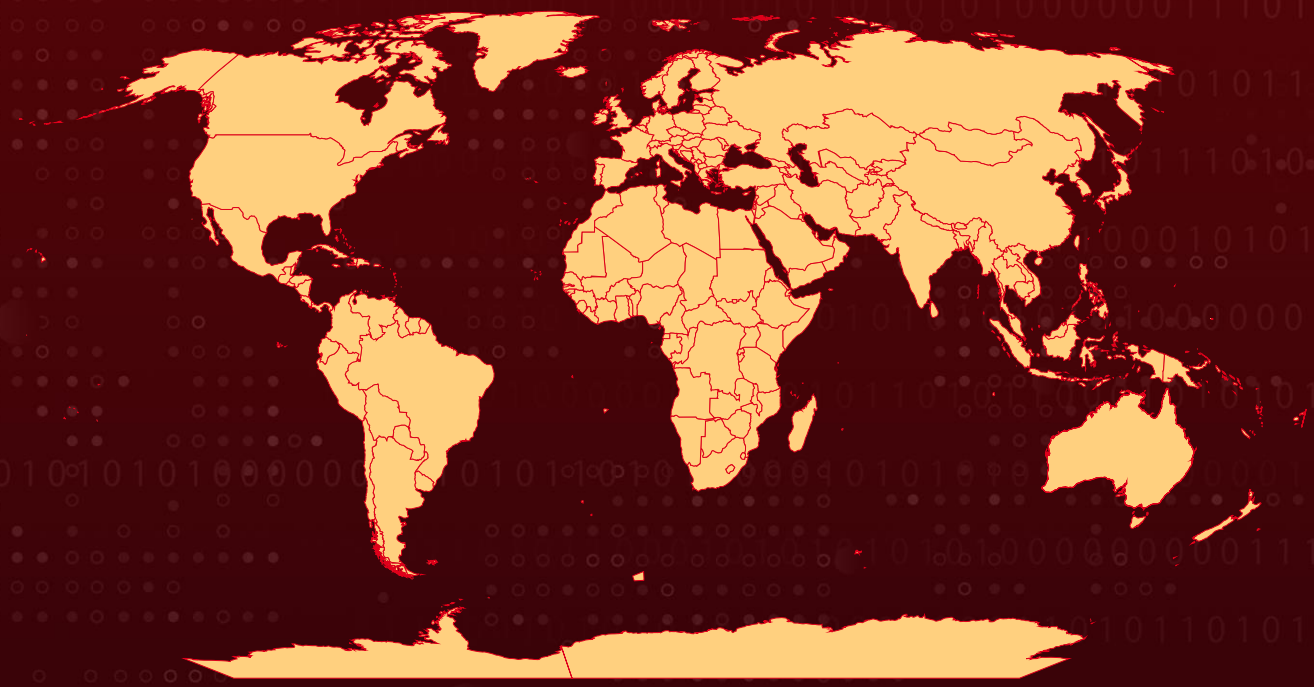
Leaked Environment Variables Fuel Cloud Data Extortion

Date of Publication	Admiralty Code	TA Number
August 20, 2024	A1	TA2024319

Summary

Affected Services: Identity Access Management (IAM), Security Token Service (STS), Simple Storage Service (S3), Simple Email Service (SES)
Targeted Regions: Worldwide
Attack: A sophisticated extortion campaign targeted cloud environments, leveraging the scalability of cloud platforms to exploit exposed environment variable files containing sensitive credentials. This operation compromised 110,000 domains, uncovering over 90,000 unique environment variables, including 7,000 access keys linked to cloud services and 1,500 associated with social media accounts.

Attack Regions



Attack Details

#1 An extortion campaign targeted cloud environments, exploiting the dynamic scalability of cloud platforms to devastating effect. The operation successfully compromised and extorted numerous victim organizations by exploiting exposed environment variable files, which contained critical information, such as application credentials.

#2 This campaign impacted 110,000 domains, exposing over 90,000 unique environment variables that held access keys or IAM credentials. Among these, 7,000 access keys were directly linked to organizations' cloud services, and 1,500 variables were tied to social media accounts.

#3 The attackers initially gained access through exposed environment files within the victim organizations' web applications. These files often store secrets, including hard-coded cloud provider access keys, SaaS API keys, and database login details, which the threat actors exploited for initial entry.

#4 After gaining access, the threat actors pivoted to the AWS Lambda service, creating a malicious Lambda function to conduct internet-wide scans of millions of domains and IP addresses. They compiled potential targets from publicly accessible third-party S3 buckets hosted in compromised cloud environments.

#5 The attackers exfiltrated data from compromised S3 buckets using the S3 Browser tool, subsequently deleting the data from the victims' buckets. They left ransom notes demanding payment in Bitcoin to prevent the stolen data from being sold.

Recommendations

Avoid Long-Lived Credentials: Replace long-lived credentials with short-lived tokens that expire after a set period and implement automated token rotation to reduce the risk of exposure. Additionally, utilize secrets management solutions, such as AWS Secrets Manager, Azure Key Vault, or HashiCorp Vault, to securely manage and rotate credentials.

Enforce Least Privilege Architecture: Apply the principle of least privilege by ensuring that users, applications, and services have only the permissions necessary for their specific roles, and regularly review and update access controls. Additionally, implement network segmentation to limit the scope of access and reduce the risk of lateral movement in the event of a breach.

Monitor and Respond: Implement continuous monitoring and logging of all cloud environments using services such as AWS CloudWatch, Azure Monitor, or Google Cloud Operations Suite to detect unusual activity and potential breaches in real time. Additionally, develop and regularly update an incident response plan that includes procedures for addressing cloud-specific threats and breaches, ensuring a swift and effective response to any security incidents.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation
TA0007 Discovery	TA0006 Credential Access	TA0010 Exfiltration	TA0040 Impact
TA0043 Reconnaissance	T1078 Valid Accounts	T1592 Gather Victim Host Information	T1136 Create Account
T1136.003 Cloud Account	T1068 Exploitation for Privilege Escalation	T1098 Account Manipulation	T1098.003 Additional Cloud Roles
T1583.007 Serverless	T1580 Cloud Infrastructure Discovery	T1526 Cloud Service Discovery	T1619 Cloud Storage Object Discovery
T1069 Permission Groups Discovery	T1069.003 Cloud Groups	T1552 Unsecured Credentials	T1552.004 Private Keys

Indicators of Compromise (IOCs)

TYPE	VALUE
URL	hxxps[:]//github[.]com/brentp/gargs/releases/download/v0[.]3[.]9/gargs_linux
SHA256	64e6ce23db74aed7c923268e953688fa5cc909cc9d1e84dd46063b62bd649bf6
IPv4	109[.]70[.]100[.]71, 144[.]172[.]118[.]62, 176[.]123[.]8[.]245, 185[.]100[.]85[.]25, 185[.]100[.]87[.]41, 185[.]220[.]101[.]190, 185[.]220[.]101[.]19, 185[.]220[.]101[.]21, 185[.]220[.]101[.]29, 185[.]220[.]101[.]30, 185[.]220[.]101[.]86, 185[.]220[.]103[.]113, 192[.]42[.]116[.]181, 192[.]42[.]116[.]187, 192[.]42[.]116[.]18, 192[.]42[.]116[.]192, 192[.]42[.]116[.]199, 192[.]42[.]116[.]201, 192[.]42[.]116[.]208, 192[.]42[.]116[.]218, 198[.]251[.]88[.]142, 199[.]249[.]230[.]161, 45[.]83[.]104[.]137, 62[.]171[.]137[.]169, 80[.]67[.]167[.]81, 89[.]234[.]157[.]254, 94[.]142[.]241[.]194, 95[.]214[.]234[.]103, 125[.]20[.]131[.]190, 196[.]112[.]184[.]14, 46[.]150[.]66[.]226, 49[.]37[.]170[.]97, 139[.]99[.]68[.]203, 141[.]95[.]89[.]92, 146[.]70[.]184[.]10,

TYPE	VALUE
IPv4	178[.]132[.]108[.]124, 193[.]42[.]98[.]65, 193[.]42[.]99[.]169, 193[.]42[.]99[.]50, 193[.]42[.]99[.]58, 195[.]158[.]248[.]220, 195[.]158[.]248[.]60, 45[.]137[.]126[.]12, 45[.]137[.]126[.]16, 45[.]137[.]126[.]18, 45[.]137[.]126[.]41, 45[.]94[.]208[.]42, 45[.]94[.]208[.]63, 45[.]94[.]208[.]76, 45[.]94[.]208[.]85, 72[.]55[.]136[.]154, 95[.]214[.]216[.]158, 95[.]214[.]217[.]173, 95[.]214[.]217[.]224, 95[.]214[.]217[.]242, 95[.]214[.]217[.]33

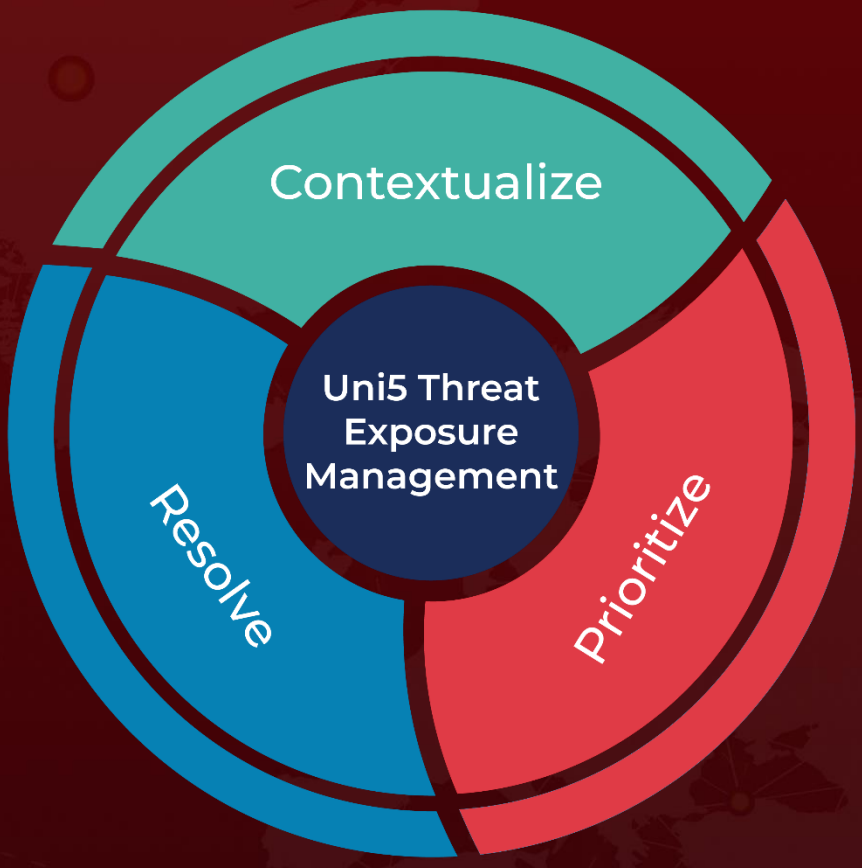
References

https://unit42.paloaltonetworks.com/large-scale-cloud-extortion-operation/

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

August 20, 2024 • 6:00 AM

More at www.hivepro.com