January 03, 2025

EC2 Grouper: A Persistent Cloud Threat Exploiting AWS Keys

Overview: Over the years, a recurring threat actor, dubbed “EC2 Grouper”, has emerged as one of the most prolific attackers targeting cloud environments. This group has been observed in numerous customer environments, leveraging automated tactics to compromise cloud identities and execute their objectives. Known for using consistent user agents and a specific security group naming convention, EC2 Grouper exemplifies the sophisticated use of cloud-native tools and APIs for reconnaissance and exploitation. This threat underscores the evolving risks posed by compromised credentials in cloud infrastructure.

CTI Analysis: EC2 Grouper employs AWS tools for PowerShell to execute their attacks, with their user agent being a notable indicator of activity. Initially, they utilized a user agent string consistent across attacks but have recently updated it to include new versioning and unusual characters, likely to evade detection. The attacker also uses a predictable security group naming pattern, such as “ec2group”, “ec2group1” up to “ec2group12345”, created via the CreateSecurityGroup API. Their modus operandi includes leveraging cloud-native APIs like DescribeInstanceTypes, DescribeRegions, and RunInstances for reconnaissance and lateral movement. Notably, their cloud activity appears largely automated, focusing on resource hijacking as the primary objective. While their end goals remain unclear, they often exploit compromised AWS keys, presumably obtained from publicly exposed repositories.

Impact Analysis: EC2 Grouper’s activities pose significant risks to cloud environments. The automated nature of their operations allows them to swiftly execute reconnaissance, create security groups, and deploy resources, resulting in potential financial losses through unauthorized resource consumption. Moreover, their focus on cloud-native APIs for lateral movement increases the risk of data breaches and infrastructure compromise. Although no manual escalation or direct objectives have been observed, the attackers’ ability to hijack

resources highlights the vulnerabilities associated with exposed credentials and insufficient monitoring.

Mitigations:

- Regularly audit code repositories for exposed credentials using tools like GitGuardian and GitHub secret scanning.
- Implement strict IAM policies with least privilege principles to limit access to sensitive APIs.
- Enable multi-factor authentication (MFA) for all cloud accounts.
- Monitor for anomalous activities, such as unusual API calls or deviations in user agent patterns.
- Deploy comprehensive Cloud Detection and Response (CDR) solutions like Lacework FortiCNAPP to detect and respond to identity compromises effectively.

Conclusion: Detecting and mitigating cloud identity compromises remains a complex challenge, especially as attackers increasingly rely on valid credentials. While indicators like user agents and security group names can assist in attribution, they are often insufficient for comprehensive threat detection. EC2 Grouper exemplifies the challenges posed by automated and sophisticated cloud attacks, emphasizing the need for robust detection strategies that focus on correlating weaker signals attackers cannot control. By adopting advanced composite alerting mechanisms and integrating cloud identity protection measures, organizations can significantly improve their detection and response capabilities, safeguarding their cloud environments against such persistent threats.

Source:

https://cybersecuritynews.com/ec2-grouper-hackers-abusing-aws-tools/

https://www.fortinet.com/blog/threat-research/catching-ec2-grouper-no-indicators-required