

**Cyber Threat Intelligence and Incident Response Report**

Incident GuardDuty ID: 1cc71b20c87252910d2ca5ab209fc698

Report Author: Christen Reinhart | Thierry Tran | Edwin Pretel | Michael Roberts

Report Date: 3/12/2024-

**INCIDENT SEVERITY**

| HIGH | MEDIUM | LOW |
| --- | --- | --- |
| **X** |  |  |

***INCIDENT DETAILS***

| ***Incident Type:*** RDP Brute Force Attack  ***Target Instance:*** IP address being targeted was 10.0.0.126.  ***Source Instance****:*  Instance ID: i-056ee78922f134039  Instance Type: t2.micro  Availability Zone: us-west-2a  ***Region:*** us-west-2a  ***Attack Vector:***  The attack was conducted via the Remote Desktop Protocol (RDP) over TCP, specifically targeting port 3389. The source instance was attempting to guess the RDP password of the target instance through brute force methods. |
| --- |

***INCIDENT DESCRIPTION***

***Summary***

| **Summary:**  An EC2 instance, identified as i-056ee78922f134039 and labeled as "BT2-Tool - OpenVPN Server1" within the "Final-401d10-v1" CloudFormation stack, has been detected performing RDP brute force attacks on the IP address 10.0.0.126 since March 13, 2024.   **Impact Analysis:**  The brute force attack represents a significant security risk, attempting unauthorized access by guessing RDP passwords. If successful, this could lead to compromised systems, unauthorized access to sensitive data, potential data breaches, and a disruption in business operations. The ongoing nature of the attack (11 hours) suggests a persistent threat, possibly indicating compromised credentials or malicious intent from within the network. The impact extends beyond just the targeted IP, potentially affecting the entire network's security posture, user trust, and regulatory compliance.  **Affected Systems/Assets:**  Primary Target: IP address 10.0.0.126 via RDP on port 3389.  Source of Attack: EC2 instance i-056ee78922f134039, part of the "Final-401d10-v1" stack, specifically used as an "OpenVPN Server1."  Network Infrastructure: Associated with VPC ID vpc-02923045326b5935e and security group "Final-401d10-v1-OpenVpnSG-P6dfwnMegVZa."  Additional Risk Areas: Given the nature of the attack, other assets within the same VPC or relying on the compromised instance for services may also be at risk. |
| --- |

***TACTICS:***

| **Initial Access [TA0001]:** The incident involving the AWS EC2 instance performing RDP brute force attacks against another system uses the TA0001 tactic, specifically under "Initial Access". This is because the attacker is attempting to gain their initial foothold within a network or system by exploiting the Remote Desktop Protocol (RDP) service. **Credential Access [TA0006]:** Performing RDP brute force attacks directly relates to the "Credential Access" tactic, specifically identified as TA0006 in the MITRE ATT&CK framework. |
| --- |

***INCIDENT TIMELINE***

| ***March 13, 2024, 01:14:21*** | Event: The system first detects outbound RDP brute force attack attempts from the EC2 instance targeting the IP address 10.0.0.126. This marks the start of the identified attack activity. |
| --- | --- |
| ***March 13, 2024, between 01:14:21 and 12:17:02*** | Event: The EC2 instance continues to perform RDP brute force attacks over this period. A total of 69 connection attempts are reported, indicating persistent attempts to gain unauthorized access through password guessing. |
| ***March 13, 2024, 12:17:02*** | Date & Time: March 13, 2024, 12:17:02  Event: The last recorded instance of the RDP brute force attack. This does not necessarily mean the end of the attack but is the last point of activity noted in the provided information. |

### 

**Cyber Kill Chain**

| **Reconnaissance** | *The attacker gathers information on targets to identify vulnerabilities and choose the method of attack. While the provided information does not explicitly mention reconnaissance, it's possible the attacker identified the EC2 instance as a viable platform for launching RDP brute force attacks through scanning or other intelligence-gathering methods.* |
| --- | --- |
| **Weaponization** | In this case, the "weapon" could be a brute force tool designed to guess RDP passwords. |
| **Delivery** | The weapon is delivered to the target. Since the attack is coming from an EC2 instance, the delivery phase might involve the compromise and utilization of this instance to launch the attack. |
| **Exploitation** | The attacker uses the weapon to exploit a vulnerability. The brute force attack attempts to exploit weak RDP passwords to gain unauthorized access. |
| **Installation** | Malware or a backdoor is installed for persistent access. None found |
| **Command & Control (C2)** | If the RDP brute force attack was successful, the attacker could use the RDP session for C2 communications. |
| **Actions on Objectives** | The specific objectives of this RDP brute force attack are not detailed, but could range from data theft to further network infiltration. |

**Documentation and Evidence:**

* The affected machine in this incident is an AWS EC2 instance with the following details:
* Instance ID: i-056ee78922f134039
* Instance Type: t2.micro
* Instance State: Running
* Availability Zone: us-west-2a
* Image ID: ami-05b626bf21fd755ee
* Image Description: OpenVPN for 401 Final
* Launch Time: March 7, 2024, 13:07:19
* Instance Tags: Named "BT2-Tool - OpenVPN Server1", associated with the CloudFormation stack "Final-401d10-v1"
* Network Interface ID: eni-0509c307aa23a6fc8
* Private IP Address: 10.0.0.176
* Public IP Address: 34.215.239.159
* Security Group ID: sg-0b23bf36ab4f201e7
* Security Group Name: Final-401d10-v1-OpenVpnSG-P6dfwnMegVZa
* This instance was involved in performing RDP brute force attacks against the IP address 10.0.0.126, utilizing the TCP protocol over port 3389. The attacks were first detected on March 13, 2024, and continued for approximately 11 hours.