SNEAK YOUR WAY TO CLOUD PERSISTENCE
- SHADOW ADMINS ARE HERE TO STAY

Asaf Hecht
Security Researcher
CyberArk
@Hechtov

Lavi Lazarovitz
Labs Team Leader
CyberArk
@LaviLazarovitz
AWS Shadow Admins

- A video frame -

The videos are available in the “Cloud Shadow Admins” blog post: https://www.cyberark.com/threat-research-blog/
AWS Shadow Admins

- Combinations of Permissions Create a Tier 0 Account
- Control Other Privileged Entities
- Hidden in Masses of Permissions and Accounts
AWS Entities

ROOT ACCOUNT

IAM

USERS

GROUPS

ROLES
Example for full “Administrator” policy:

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "*",
      "Resource": "*"
    }
  ]
}
```

or “Deny”
or any other actions from thousands of options
or any other available AWS resources
Policy 2 - also Full Admin - Shadow Admin

```
"Statement": [
  {
    "Sid": "ShadowPolicy",
    "Effect": "Allow",
    "Action": [
      "iam:CreateInstanceProfile",
      "iam:PassRole",
      "iam:AddRoleToInstanceProfile",
      "ec2:AssociateIamInstanceProfile"
    ],
    "Resource": [
      "arn:aws:iam::*:instance-profile/**",
      "arn:aws:iam::*:role/**",
      "arn:aws:ec2::*:instance/**"
    ]
  }
]
```
SNEAKY PERSISTENCE AND ESCALATION VECTORS

10 Sets of Permissions You Should Search and Control
IAM Sensitive Permissions to Follow

IAM -> Sensitive API Permission Categories

- Groups
- Credentials
- Permission Policies
- Roles
(1) Permission to: AddUserToGroup

Malicious User

Admin Group

+1
AddUserToGroup

Adds the specified user to the specified group.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters.

GroupName

The name of the group to update.

This parameter allows (per its regex pattern) a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: _+\-,@-

Type: String


Pattern: \{\+\+,\-,\@-\}

Required: Yes

UserName

The name of the user to add.

This parameter allows (per its regex pattern) a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: _+\-,@-

Type: String


Pattern: \{\+\+,\-,\@-\}
AddUserToGroup API Call

AWS CLI

```bash
>aws iam add-user-to-group --group-name Admin_Group --username Attacker_User
```
Newly Added
Jumping Forward to the Credentials Category

Credentials

- Web Login
- Password
- Programmatically
- Access Key
(2) Permission to: CreateAccessKey

- A video frame -

The videos are available in the “Cloud Shadow Admins” blog post: https://www.cyberark.com/threat-research-blog/
(3) Permissions to: Attach*Policy

Users + Groups + Privileged Permission Policy =}

Roles
(4) Permissions to: *PolicyVersion
Modifying Policy Versions

- A video frame -

The videos are available in the “Cloud Shadow Admins” blog post: https://www.cyberark.com/threat-research-blog/
Modifying Policy Versions

The Target Policy Name

The New Permissions

The New Version
(5) Permissions to: *InstanceProfile

Privileged Role + EC2 Instance = Attacker

Like the Opening Demo
# IAM Sensitive Permissions to Follow

<table>
<thead>
<tr>
<th>Category</th>
<th>API specific permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Groups</td>
<td>(1) AddUserToGroup</td>
</tr>
<tr>
<td>Credentials</td>
<td>(2) CreateAccessKey</td>
</tr>
<tr>
<td></td>
<td>(3) CreateLoginProfile</td>
</tr>
<tr>
<td></td>
<td>(4) UpdateLoginProfile</td>
</tr>
</tbody>
</table>
| Permission policies| (5) AttachUserPolicy  
|                   |  AttachGroupPolicy                                          |
|                   |  AttachRolePolicy                                           |
|                   | (6) PutUserPolicy                                          |
|                   |  PutGroupPolicy                                             |
|                   |  PutRolePolicy                                              |
|                   | (7) CreatePolicy                                            |
|                   | (8) CreatePolicyVersion  
|                   |  SetDefaultPolicyVersion                                   |
| Roles             | (9) PassRole  
|                   |  CreateInstanceProfile                                     |
|                   |  AddRoleToInstanceProfile                                  |
|                   | (10) UpdateAssumeRolePolicy                                |
Hiding The Shadow Admins

- Use benign names: “readOnly”
- Attach permissions to legitimate group
- Deny read access to account
AWS Shadow Admins
Detection & Mitigation
Detection & Mitigation

AWS\textit{stealth}
Identify Existing Shadow Admins

Remove Shadow Admins Privileges

AWS\textit{trace}
Identify Shadow Admins Activity

Secure Shadow Admins Credentials / MFA

CYBERARK

RSAConference2018
SkyArk: Free Cloud Security Project

Publish - Today

Scans AWS entities
Needs Read Only Access
Discovers Shadow Admins

https://github.com/cyberark/SkyArk
SkyArk \ AWStealth - Demo
Discovering AWS Shadow Admins
SkyArk: Free Cloud Security Project

Scans AWS logs | Needs Read Only Access | Identifies Sensitive Activities

https://github.com/cyberark/SkyArk
SkyArk \ AWStrace - Demo
Analyzing AWS CloudTrail Logs
GuideLights

Shadow Admins: Specific Privileged Permissions

Discover privileged Shadow Admins using “SkyArk”

Contain the Attack Surface by Removing Permissions and Using Conditional Policies
Actionable Takeaways

1. Scan your environments for AWS Shadow Admins:
   - SkyArk\AWStealth

2. Monitor for sensitive permission actions:
   - SkyArk\AWStrace
   - Configure automatic alerts on permission changes

3. Remove Shadow Admins sensitive permissions where possible

4. Secure Cloud Admin accounts:
   - MFA
   - Credentials management
References

- **SkyArk** - free mitigation tool, available in GitHub:
  
  [https://github.com/cyberark/SkyArk](https://github.com/cyberark/SkyArk)

- **AWS Shadow Admins - Blogpost**:
  
  [https://www.cyberark.com/threat-research-blog/](https://www.cyberark.com/threat-research-blog/)

- **AWS Official links**:
  
  - AWS Security Center:
    [https://aws.amazon.com/security/](https://aws.amazon.com/security/)
  
  - AWS IAM User Guide:
  
  - AWS IAM API References:
    [https://docs.aws.amazon.com/IAM/latest/APIReference/Welcome.html](https://docs.aws.amazon.com/IAM/latest/APIReference/Welcome.html)
  
  - AWS CloudTrail User Guide:
GREAT... ANY Q? WE WILL TRY TO A

Also, follow us for more updates and fun:

Lavi.Lazarovitz@cyberark.com, @LaviLazarovitz
Asaf.Hecht@cyberark.com, @Hechtov