ATTACK DETECTION FUNDAMENTALS: AZURE

Masande Mtintsilana
C:\> whoami /all

Masande Mtintsilana – Senior Security Consultant
GOALS OF THIS SERIES

• Help improve understanding of attacks, so we can detect and prevent them

• Demonstrate attack detection fundamentals and understand how enterprise products work under the hood
HOW?

- **Analyse** set of known TTPs used by real threat actors
- **Emulate** them in a controlled lab environment
- **Observe** the traces that they leave
HOW?

- *Simple* lab setup
- *Open-source* offensive and defensive tools
- *Lab scripts* provided
SERIES OVERVIEW

WINDOWS
07/04/2021
16:00-17:00 BST

MACOS
14/04/2021
16:00-17:00 BST

AWS
21/04/2021
16:00-17:00 BST

AZURE
28/04/2021
16:00-17:00 BST

You are here!
WORKSHOP #4: AZURE

• **Practical Walk-through** of an end-to-end attack in an Azure environment

• Highlight the different **log sources** and **log events** provided by Azure

• Discuss **Detection Opportunities** and **Challenges** that are relevant to the cloud in general.
AGENDA

Consent Phishing

Initial Access

Hunting for Credentials

Internal Recon

Abusing Legitimate Features

Defense Evasion

Abusing Legitimate features...again

Lateral Movement
LAB SETUP

Subscription

Resource Group

Azure VM (target-vm)

Logic Apps (resource-tracker)

Azure VM (attack-vm)

Logs

Log Analytics Workspace

Azure AD
TELEMETRY SOURCES

- **Azure Active Directory Logs**
  - Sign-in Activity
  - Audit Activity

- **Activity Logs (Control Plane)**
  - Subscription-level events

- **Resource Logs (Data Plane)**
  - Windows Event Logs
  - Storage Analytics logs

- **Network Logs**
  - NSG Flow Logs
Lab 1 – Gaining a foothold with Consent Phishing

Lab 2 – Hunting for Credentials

Lab 3 – Lateral Movement and Defense Evasion
INITIAL ACCESS WITH CONSENT PHISHING
Azure Active Directory (Azure AD) is Microsoft’s cloud-based identity and access management service.

- Provides SSO for many of Microsoft’s services (Azure Cloud, O365, etc)
- Stores useful information about users:
  - Name
  - Department
  - Email address
**AZURE AD SINGLE-TENANT APP**

- **App Registration** - A template that describes your application:
  - Name
  - Permissions needed
  - Credentials

- **Enterprise Application/Service Principal** – An instance of your application in Azure AD. Created during registration

**Portal Terminology** (PowerShell Terminology)

Screenshot source: https://www.sebbiaan.com/the-difference-between-azuread-app-registrations-and-enterprise-applications-explained/
AZURE AD MULTI-TENANT APP

Org X

Azure Active Directory
Tenant #1

Instance of

App Registration
(Application)

Reference to

Enterprise Application
(Service Principal)

Org Y

Azure Active Directory
Tenant #2

Enterprise Application
(Service Principal)

Portal Terminology
(PowerShell Terminology)

Screenshot source: https://www.seb8iaan.com/the-difference-between-azuread-app-registrations-and-enterprise-applications-explained/
AZURE AD CONSENT FRAMEWORK

- Provides a frontend to the **Consent Grant Flow**

- User is provided with:
  - Application name
  - Organisation name
  - Permission requested

- In the background, third party SPN is registered in your Azure AD tenant
## Enterprise Applications

![Enterprise Applications](image)

### New application
- **Application type:** All Applications
- **Applications status:** Any
- **Application visibility:** Any

### Applications
- **AAD Request Verification Service - PROD**
- **AI Graph Client**
- **Application Insights Configuration Service**
- **Azure Cost Management XCloud**
- **Azure Database for PostgreSQL Merlin**
- **Azure Search Management**
- **Azure Spring Cloud Domain Management**
- **Azure Storage**
- **Azure VPN**
- **https://www.microsoft.com**
CONSENT PHISHING

O365 ATTACK TOOLKIT

A toolkit that “allows operators to perform OAuth phishing attacks.”

- Provides “external server “that monitor for users who have been successfully phished
- Provides Management interface to easily perform data exfil.

https://github.com/mdsecactivebreach/o365-attack-toolkit
LAB: CONSENT PHISHING
DEMO 1: CONSENT PHISHING

https://www.youtube.com/watch?v=fWlyYLcozvo
PREVENTING CONSENT PHISHING

1. Do not allow user consent
   An administrator will be required for all apps.

2. Allow user consent for apps from verified publishers, for selected permissions (Recommended)
   All users can consent for permissions classified as "low impact", for apps from verified publishers or apps registered in this organization.

3. Allow user consent for apps
   All users can consent for any app to access the organization's data.
# AZURE AD LOGS

## Sign-in Logs

<table>
<thead>
<tr>
<th>Date</th>
<th>Original Request</th>
<th>User</th>
<th>Application</th>
<th>Status</th>
<th>IP address</th>
<th>Location</th>
<th>Conditional a...</th>
</tr>
</thead>
<tbody>
<tr>
<td>10/15/2019, 4:00:...</td>
<td>3b849c9a-1671-...</td>
<td>Timothy Perkins</td>
<td>Azure Portal</td>
<td>Success</td>
<td>167.220.2.8</td>
<td>Redmond, Wash...</td>
<td>Not Applied</td>
</tr>
<tr>
<td>10/15/2019, 3:55:...</td>
<td>ebcaccd4-c7cf-4...</td>
<td>Timothy Perkins</td>
<td>Kusto Web Expl...</td>
<td>Success</td>
<td>131.107.147.47</td>
<td>Redmond, Wash...</td>
<td>Not Applied</td>
</tr>
<tr>
<td>10/15/2019, 3:55:...</td>
<td>b2b6a4fa-a726-...</td>
<td>Timothy Perkins</td>
<td>Kusto Web Expl...</td>
<td>Success</td>
<td>131.107.147.47</td>
<td>Redmond, Wash...</td>
<td>Not Applied</td>
</tr>
</tbody>
</table>

## Audit Logs

<table>
<thead>
<tr>
<th>Date</th>
<th>Service</th>
<th>Category</th>
<th>Activity</th>
<th>Status</th>
<th>Target(s)</th>
<th>Initiated by (Actor)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2/7/2019, 2:16:33 AM</td>
<td>Core Directory</td>
<td>Policy</td>
<td>Delete policy</td>
<td>Success</td>
<td>MFA Registration</td>
<td><a href="mailto:admin@aad171.ccsc.com">admin@aad171.ccsc.com</a></td>
</tr>
<tr>
<td>2/7/2019, 2:16:33 AM</td>
<td>Core Directory</td>
<td>Policy</td>
<td>Delete policy</td>
<td>Success</td>
<td>02/07/2019 10:15 AM</td>
<td><a href="mailto:admin@aad171.ccsc.com">admin@aad171.ccsc.com</a></td>
</tr>
<tr>
<td>2/7/2019, 2:15:56 AM</td>
<td>Identity Protection</td>
<td>Policy</td>
<td>Set MFA registration policy</td>
<td>Failure</td>
<td>Test_Test_aad171</td>
<td><a href="mailto:admin@aad171.ccsc.com">admin@aad171.ccsc.com</a></td>
</tr>
<tr>
<td>2/7/2019, 2:15:56 AM</td>
<td>Core Directory</td>
<td>Policy</td>
<td>Add policy</td>
<td>Failure</td>
<td>MFA Registration</td>
<td>Azure AD Identity Protection</td>
</tr>
</tbody>
</table>
DEMO 2: CONSENT PHISHING LOGS

https://www.youtube.com/watch?v=5MseIR55jYg
CONSENT GRANT LOG EVENTS

Add SPN
O365 toolkit SPN added to victim Tenant

Delegate Permission Grant
Application assigned permissions to access exchange, sharepoint, etc

Add App Role Assignment
User is assigned app role defined by application

Consent to application
Application has been consented 😊
NATIVE DETECTION CAPABILITIES

Microsoft Cloud App Security
Azure Sentinel
Azure Workbooks
Azure Alerts
HUNTING FOR CREDENTIALS
COMMON OFFENDERS

- Azure Functions
- Azure Automation Runbooks
- Azure Logic Apps
AZURE FUNCTION APPS

Azure Functions

Get function URL

Key: default
URL: https://myfunctionapp.azurewebsite...
AZURE LOGIC APPS

Azure Logic Apps
AUTOMATING CREDENTIAL HUNTING

- Microburst has `Get-AzPasswords` that covers services:
  - Key Vault
  - Automation accounts
- Focusing on what we can get with limited privs

https://github.com/NetSPI/MicroBurst
LAB 2: HUNTING FOR CREDENTIALS
DEMO 3: CREDENTIAL HUNTING

https://www.youtube.com/watch?v=RIcITc8o_jc
<table>
<thead>
<tr>
<th>Activity log</th>
<th>Subscription</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provides insight into the operations on each Azure resource in the subscription from the outside (the management plane) in addition to updates on Service Health events. Use the Activity Log to determine the what, who, and when for any write operations (PUT, POST, DELETE) taken on the resources in your subscription. There is a single Activity log for each Azure subscription.</td>
<td></td>
</tr>
</tbody>
</table>

The activity log contains all write operations (PUT, POST, DELETE) performed on your resources. It does not include read operations (GET). You can use the audit logs to find an error when troubleshooting or to monitor how a user in your organization modified a resource.

Note: Activity logs are retained for 90 days. You can query for any range of dates, as long as the starting date is not more than 90 days in the past.
CAN WE DETECT THIS?

- Service Principals are likely to be predictable:
  - Fixed set of operations
  - **Fixed Locations**

<table>
<thead>
<tr>
<th>AppId</th>
<th>deced9e69-4e9d-4670-8bcb-b109ae30b57</th>
</tr>
</thead>
<tbody>
<tr>
<td>Id</td>
<td>de9b6bad-d1b6-4c59-852f-928697cc6d00</td>
</tr>
<tr>
<td>IPAddress</td>
<td>86.151.58.213</td>
</tr>
<tr>
<td>LocationDetails</td>
<td>(&quot;city&quot;: &quot;Lambeth&quot;, &quot;state&quot;: &quot;Greater London&quot;, &quot;countryOrRegion&quot;: &quot;GB&quot;, &quot;geoCoordinates&quot;: {&quot;latitude&quot;: 51.4583282, 47.0703, &quot;longitude&quot;: 0.114169999957085})</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ResourceDisplayName</th>
<th>Windows Azure Service Management API</th>
</tr>
</thead>
<tbody>
<tr>
<td>ResourceId</td>
<td>797f4846-ba00-4df7-ba43-da1f8f63013</td>
</tr>
<tr>
<td>ServicePrincipalId</td>
<td>14e938dc-6a54-45d7-89eb-0407c948732a</td>
</tr>
<tr>
<td>ServicePrincipalName</td>
<td>resource-tracker-app</td>
</tr>
<tr>
<td>Type</td>
<td>AADServicePrincipalSigninLogs</td>
</tr>
</tbody>
</table>
LATERAL MOVEMENT AND DEFENSE EVASION
GOT PRIVILEGED ACCESS. NOW WHAT?

Objectives:

- PII
- Financial data
- Intellectual Property
LATERAL MOVEMENT

Deploy SSH Key

**Azure CLI**

```
az vm create
  --resource-group myResourceGroup
  --name myVM
  --image UbuntuLTS
  --admin-username azureuser
  --ssh-key-values mysshkey.pub
```

Deploy Custom Script Extension

**Azure CLI**

```
az vm extension set
  --resource-group myResourceGroup
  --vm-name myVM --name customScript
  --publisher Microsoft.Azure.Extensions
  --settings ./script-config.json
```

Invoke Run-Command

**Azure CLI**

```
az vm run-command invoke
  --command-id
  [--ids]
  [--name]
  [--parameters]
  [--resource-group]
  [--scripts]
  [--subscription]
```
MOVING LATERALLY WITH STEALTH

• Org likely to continue doing what they do well.

• **Goal:** Not setting off alarm-bells in data plane (e.g. EDR, Defender, etc)

• **How:** not running any code on target VMs
- Composed of:
  - VM
  - Disks
  - Network Interface
  - Public IP Address
MOVING LATERALLY WITH STEALTH

1. Snapshot VM OS Disk
2. Create new Managed Disk
3. Deploy attacker VM
4. Mount OS Disk as a data disk
DEMO 4: MOVING LATERALLY

https://www.youtube.com/watch?v=M2KMUKfZCFc
DEMO 5: MOVING LATERALLY LOGS

https://www.youtube.com/watch?v=Uel59pJ0yXs
### Monitoring

**1. Create a Snapshot**

<table>
<thead>
<tr>
<th>Time</th>
<th>Activity 1</th>
<th>Activity 2</th>
<th>Event Type</th>
<th>Resource</th>
</tr>
</thead>
<tbody>
<tr>
<td>4/19/2021, 11:33:44.673 PM</td>
<td>AzureActivity</td>
<td>AzureActivity</td>
<td>Create or Update Virtual Machine</td>
<td>Microsoft.Compute.VirtualMachines/write</td>
</tr>
<tr>
<td>4/19/2021, 11:33:38.534 PM</td>
<td>AzureActivity</td>
<td>AzureActivity</td>
<td>Create or Update Virtual Machine</td>
<td>Microsoft.Compute.VirtualMachines/write</td>
</tr>
<tr>
<td>4/19/2021, 11:33:38.509 PM</td>
<td>AzureActivity</td>
<td>AzureActivity</td>
<td>‘auditIfNotExists’ Policy action.</td>
<td>Microsoft.Authorization/policies/auditIfNotExists/action</td>
</tr>
<tr>
<td>4/19/2021, 11:33:38.024 PM</td>
<td>AzureActivity</td>
<td>AzureActivity</td>
<td>Create or Update Virtual Machine</td>
<td>Microsoft.Compute.VirtualMachines/write</td>
</tr>
<tr>
<td>4/19/2021, 11:33:19.003 PM</td>
<td>AzureActivity</td>
<td>AzureActivity</td>
<td>Create or Update Disk</td>
<td>Microsoft.Compute/disks/write</td>
</tr>
<tr>
<td>4/19/2021, 11:33:13.329 PM</td>
<td>AzureActivity</td>
<td>AzureActivity</td>
<td>Create or Update Disk</td>
<td>Microsoft.Compute/disks/write</td>
</tr>
<tr>
<td>4/19/2021, 11:33:13.149 PM</td>
<td>AzureActivity</td>
<td>AzureActivity</td>
<td>Create or Update Disk</td>
<td>Microsoft.Compute/disks/write</td>
</tr>
<tr>
<td>4/19/2021, 11:33:04.286 PM</td>
<td>AzureActivity</td>
<td>AzureActivity</td>
<td>Create or Update Snapshot</td>
<td>Microsoft.Compute/snapshots/write</td>
</tr>
<tr>
<td>4/19/2021, 11:32:58.757 PM</td>
<td>AzureActivity</td>
<td>AzureActivity</td>
<td>Create or Update Snapshot</td>
<td>Microsoft.Compute/snapshots/write</td>
</tr>
</tbody>
</table>
## MONITORING

2. Create a Managed Disk

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Activity Type</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>4/19/2021, 11:33:44.673 PM</td>
<td>AzureActivity</td>
<td>Create or Update Virtual Machine</td>
<td>Microsoft.Compute.VirtualMachines/write</td>
</tr>
<tr>
<td>4/19/2021, 11:33:38.524 PM</td>
<td>AzureActivity</td>
<td>Create or Update Virtual Machine</td>
<td>Microsoft.Compute.VirtualMachines/write</td>
</tr>
<tr>
<td>4/19/2021, 11:33:38.509 PM</td>
<td>AzureActivity</td>
<td>'auditIfNotExists' Policy action.</td>
<td>Microsoft.Authorization/policies/auditIfNotExists/action</td>
</tr>
</tbody>
</table>
3. Attach disk to attacker VM

<table>
<thead>
<tr>
<th>Date/Time</th>
<th>Activity 1</th>
<th>Activity 2</th>
<th>Description</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>4/19/2021, 11:33:44 PM</td>
<td>AzureActivity</td>
<td>AzureActivity</td>
<td>Create or Update Virtual Machine</td>
<td>Microsoft.ComputeVirtualMachines/write</td>
</tr>
<tr>
<td>4/19/2021, 11:33:38 PM</td>
<td>AzureActivity</td>
<td>AzureActivity</td>
<td>Create or Update Virtual Machine</td>
<td>Microsoft.ComputeVirtualMachines/write</td>
</tr>
<tr>
<td>4/19/2021, 11:33:38 PM</td>
<td>AzureActivity</td>
<td>AzureActivity</td>
<td>‘auditIfNotExists’ Policy action.</td>
<td>Microsoft.Authorization/policies/auditIfNotExists/action</td>
</tr>
<tr>
<td>4/19/2021, 11:33:38 PM</td>
<td>AzureActivity</td>
<td>AzureActivity</td>
<td>Create or Update Virtual Machine</td>
<td>Microsoft.ComputeVirtualMachines/write</td>
</tr>
<tr>
<td>4/19/2021, 11:33:19 PM</td>
<td>AzureActivity</td>
<td>AzureActivity</td>
<td>Create or Update Disk</td>
<td>Microsoft.Compute/disks/write</td>
</tr>
<tr>
<td>4/19/2021, 11:33:13 PM</td>
<td>AzureActivity</td>
<td>AzureActivity</td>
<td>Create or Update Disk</td>
<td>Microsoft.Compute/disks/write</td>
</tr>
<tr>
<td>4/19/2021, 11:33:13 PM</td>
<td>AzureActivity</td>
<td>AzureActivity</td>
<td>Create or Update Disk</td>
<td>Microsoft.Compute/disks/write</td>
</tr>
<tr>
<td>4/19/2021, 11:33:04 PM</td>
<td>AzureActivity</td>
<td>AzureActivity</td>
<td>Create or Update Snapshot</td>
<td>Microsoft.Compute/snapshots/write</td>
</tr>
<tr>
<td>4/19/2021, 11:32:58 PM</td>
<td>AzureActivity</td>
<td>AzureActivity</td>
<td>Create or Update Snapshot</td>
<td>Microsoft.Compute/snapshots/write</td>
</tr>
</tbody>
</table>
CONCLUSIONS
CONCLUSION

Attack Simulation provides useful Insights

Cloud Detection Can Be Tricky

Understand what *normal* looks like in *your* environment

Keep Track of Your High Privileged Service Principals