AWS CloudFormation Template - Malware Analysis

This template is designed to spin up a temporary malware analysis platform and all its required resources in AWS. Once the environment has been created by Cloudformation, the new system will pull over a powershell script and install all required software.

Requirements

AWS administrator must have a valid Virtual Private Cloud (VPC) created. Make sure that you note the VPC ID (ex: vpc-12345678) and subnet.

Template Details

This template uses the latest `Microsoft Windows Server 2019 Base` for your respective region. This stack will create:

- EC2 Instance (virtual machine)
- Subnet
- Security Group
- CloudWatch Alarm

AWS CloudWatch Alarm

This template contains a CloudWatch Alarm to trigger the shutdown of the instance if the CPU utilization goes below 10.0%, three times, within a 15 minute period. This function is designed to keep costs down post analysis. To use this function, the account executing the CloudFormation template must have proper permissions. Here is an example JSON IAM permissions template:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "cloudwatch:DescribeAlarms",
                "ec2:DescribeInstanceStatus",
                "ec2:DescribeInstances",
                "ec2:DescribeSnapshots",
                "ec2:DescribeVolumeStatus",
                "ec2:DescribeVolumes",
                "ec2:RebootInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances",
                "ec2:CreateSnapshot"
            ],
            "Resource": "*"
        }
        ]
    }
```

You can remove this function from the template by deleting the **REWorkstationAlarm** resource from the template.

Creating a Stack

1. Navagate to the AWS CloudFormation site.
2. Choose **Upload a template to Amazon S3** and choose **malware-re.yaml**.
3. Click Next.
4. Fill in a unique name for `Stack name`.
5. Set the password and username for `AdminPassword` and `AdminUser` respectively.
6. Choose the `InstanceType` based on your requirements. Note that you will be charged for larger deployments.
7. Choose the `KeyName` you wish to use for this deployment.
8. Leave the value in `LatestAmiId`.
9. Enter a network CIDR block that fits within the CIDR block of your VPC. For example, a VPC with a CIDR block of 10.10.0.0/16; a CIDR block for this entry could be 10.10.1.0/24.
10. If you would like to restrict the ingress into this system to a network or specific IP address, enter it here. For example, if my public IP address was 12.34.56.78, this entry would be **12.34.56.78/32**.
11. Enter your VPC ID for `VPC`.
12. Click Next, Next, then Create

Ensure that you monitor the `Events` tab for any errors in deployment. Once the stack is deployed, you will have to wait for the users to be created and the software to be installed. This process will take approximately **15 minutes**.

Installed software

Package	Purpose	Site
Chrome Browser	Anything other than IE	https://www.google.com/chrome/
Detect-It-Easy	Program to determine types of files	https://github.com/horsicq/Detect-It-Easy
Python 2.7 & PIP	Python programming language	https://www.python.org/
Ghidra	Software reverse engineering tool developed by the US NSA	https://ghidra-sre.org/
HxD	Hex Editor	https://mh-nexus.de/en/hxd/
IDA Free v7	Interactive Dissassembler by Hex Rays	https://out7.hex-rays.com

Package	Purpose	Site
PEStudio	Software for analyzing Windows PE files	https://www.winitor.com
Volatility	Memory analysis software written in Python	https://github.com/volatilityfoundation/volatility
Visual Studio Code	Text editor	https://code.visualstudio.com/
x64dbg	Open source debugger	https://x64dbg.com/#start

Legal and Disclaimers

The author is not responsible for any unforseen effects during deployment or while using the instance. Analyze and reverse at your own risk!