Note: You are viewing an old, archived version of this content. The latest version is available in the 'main' branch.

ADWS Connection from Unexpected Binary

Metadata

ID: ADWS_Connection_from_Unexpected_Binary-Win

OS: WindowsEndpoint, WindowsServer

FP Rate: Medium

ATT&CK Tags

Tactic	Technique	Subtechnique	Technique Name
TA0009 - Collection	T1119		Automated Collection
TA0007 - Discovery	T1087	002	Account Discovery - Domain Account

Utilized Data Sources

Log Provider	Event ID	Event Name	ATT&CK Data Source	ATT&CK Data Component
MicrosoftThreatProtection	ConnectionSuccess		Network Traffic	Network Connection Creation

Technical description of the attack

This query first collects the IP addresses of all machines that have the Active Directory Web Services (ADWS) service running. It then searches for network connections to these IP addresses from processes that are not expected to connect to ADWS.

Permission required to execute the technique

User

Detection description

ADWS is a Windows service that allows Active Directory to be queried via a web service. While this service is not malicious by itself, it can be used by attackers to query Active Directory from compromised machines.

Considerations

ADWS is the protocol used by the Active Directory PowerShell module. Therefore, connections from PowerShell to ADWS are expected. The query relies on the fact that both the domain controller running the ADWS service and the client from which the connection is made are enrolled in Microsoft Defender for Endpoint.

False Positives

ADWS is used by a number of legitimate applications that need to interact with Active Directory. These applications should be added to the allow-listing to avoid false positives.

Suggested Response Actions

Investigate the suspicious connection:

- Is the process that made the connection expected to connect to ADWS?
- Are there any other signs of compromise on the affected machine?

Detection Blind Spots

An attacker might inject code into a legitimate process and use that process to connect to ADWS.

References

- https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/dd391908(v=ws.10)

Detection

Language: Kusto

Platform: M365 Security

Query:

```
let timeframe = 2*1h;
let ADWSIPs=(
    DeviceNetworkEvents
    | where ingestion_time() >= ago(timeframe)
    | where InitiatingProcessFolderPath == @"c:\windows\adws\microsoft.a
    | where LocalPort == 9389
    | distinct LocalIP
);
DeviceNetworkEvents
| where ingestion_time() >= ago(timeframe)
| where ActionType == "ConnectionSuccess"
| where RemotePort == 9389
| where RemoteIP in (ADWSIPs)
| where not(isempty(InitiatingProcessFileName))
| where not(InitiatingProcessFolderPath in~ (@"c:\windows\system32\dsac.
| where not(InitiatingProcessFolderPath startswith @"c:\windows\system32
| where not(InitiatingProcessFolderPath startswith @"c:\windows\syswow64
| where not(InitiatingProcessFolderPath startswith @"c:\program files\mi
```

```
// Begin environment-specific filter.
// End environment-specific filter.
```

Version History

Version	Date	Impact	Notes
1.1	2024-01-15	minor	Publish this as part of new FalconFriday blog.
1.0	2023-11-27	major	Initial version.