CAR-2016-04-005: Remote Desktop Logon

A remote desktop logon, through RDP, may be typical of a system administrator or IT support, but only from select workstations. Monitoring remote desktop logons and comparing to known/approved originating systems can detect lateral movement of an adversary.

Submission Date: 2016/04/19
Update Date:
Information Domain: Host
Data Subtypes: Login
Analytic Type: Situational Awareness
Applicable Platforms: Windows
Contributors: MITRE/NSA

ATT&CK Detections

Technique	Subtechnique(s)	Tactic(s)	Level of Coverage
Remote Services	Remote Desktop Protocol	Lateral Movement	Moderate

D3FEND Techniques

ID	Name
D3-RTSD	Remote Terminal Session Detection

Implementations

Pseudocode

Look in the system logs for remote logons using RDP.

```
[EventCode] == 4624 and
[AuthenticationPackageName] == 'Negotiate' and
[Severity] == "Information" and
[LogonType] == 10
```

Sigma

Sigma version of the above pseudocode, with some modifications.

Logpoint, LogPoint native

LogPoint version of the above pseudocode.

```
norm_id=WinServer event_id=4624 package="Negotiate" log_level="INFO" logon_type=10
```