Cyber Security
Snapshot

Exploring and Assessing Current Topics
MICHIGAN CYBER COMMAND CENTER (MC3)

March 14, 2019
CS-03-2019

REMOTE DESKTOP PROTOCOL (RDP)

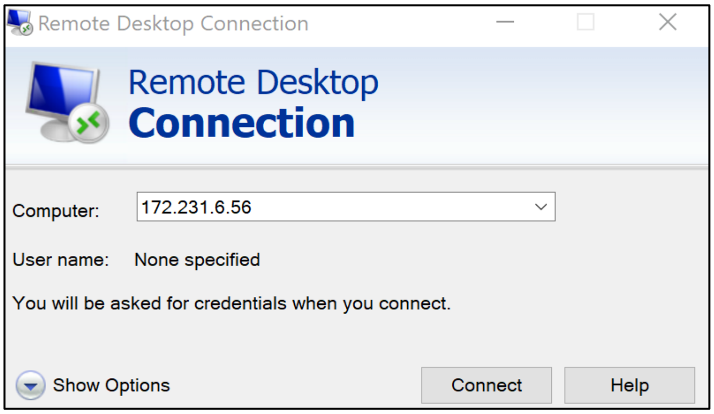
OVERVIEW

The MC3 is aware of multiple incidents within Michigan where attacks were initialized by using Remote Desktop Protocol (RDP) connections. Many of these attacks lead to ransomware infections resulting in data being encrypted. RDP attacks continue to be a favorable attack vector for malicious actors.

RDP APPLICATION

RDP, formerly known as Terminal Services Client, is an encrypted communication method which allows a user to remotely access a computer via a Graphical User Interface (GUI). RDP is a built in Microsoft protocol to Windows operating systems. RDP clients exist for Microsoft, MacOS, Linux, Unix, and various mobile operating systems. RDP can be used to exfiltrate data, reconfigure systems, or inject malware on a system, allowing other forms of remote control/communication.

RDP has legitimate business uses including remote support or control of systems. Remote access may be needed to avoid traveling distances to physically access a system. Administrators and users need to be aware of the security risks associated with RDP being enabled. With proper configurations, RDP can be instituted safely.



Computer: 172.231.6.56

User name: None specified

You will be asked for credentials when you connect.

Figure 1: RDP connection interface.

SECURITY CONCERNS

Malicious actors frequently target machines with RDP enabled, typically on port 3389. Default settings allow an unlimited number of authentication attempts, thus susceptible to brute-force attacks. Weak or common dictionary passwords can quickly be guessed with this attack vector. By default, when logging in over RDP the account will have administrative rights, thus compounding the problem. Outdated versions of RDP can allow for man-in-the-middle attacks. Publicly available RDP ports can be located using tools such as Shodan. Some RDP credentials are available for sale on the dark web.

Properly configuring RDP on a network can greatly reduce the risk of a successful RDP attack.

This document is the property of the Michigan Cyber Command Center (MC3) and is prepared for the limited purpose of information sharing. The information is designated UNCLASSIFIED/TLP WHITE. ***Information found within this document can be shared without restriction. This document must not be reclassified in any way, in whole or in part. Violation of this restriction will be cause from removal from MC3 distribution lists.***

RDP CONFIGURATION CONSIDERATIONS

Organizations should know if RDP is enabled on their devices. RDP should be disabled on any device where there is no business need for it. The default port can be changed to slow the identification of an open RDP port. The primary defense to prevent a successful RDP attack is the use of strong passwords. The MC3 recommends a minimum 15-character, complex (non-dictionary) password/passphrase for any account which RDP access is enabled.

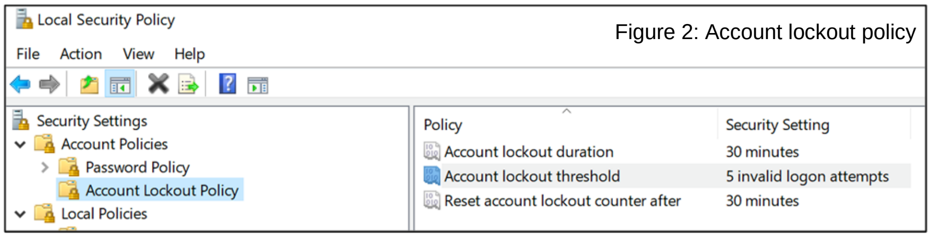


Figure 2: Account lockout policy

Policy	Security Setting
Account lockout duration	30 minutes
Account lockout threshold	5 invalid logon attempts
Reset account lockout counter after	30 minutes

RDP should be configured to prevent unlimited authentication attempts. All RDP authentications should be logged and forwarded on to a central log server in case access is obtained and logs are cleared. Administrators should review all RDP authentication activity on a routine basis. To increase security, RDP can be configured behind a firewall with access only through a VPN connection to the local network. As with all software, keeping RDP updated to the current version can be a vital defense.

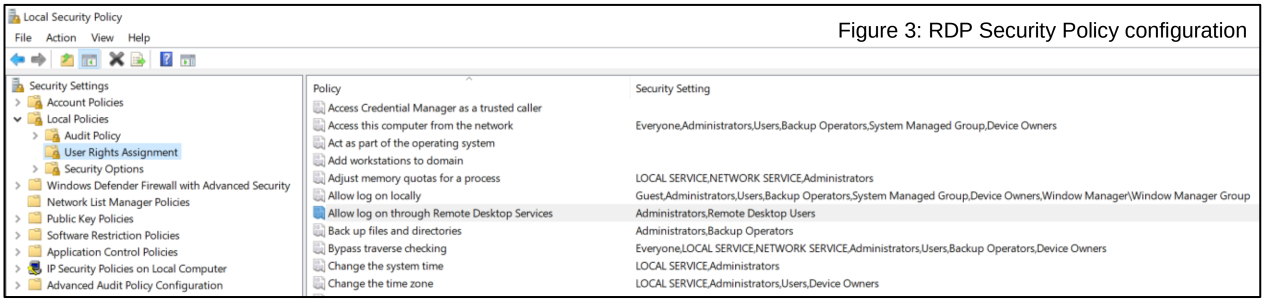


Figure 3: RDP Security Policy configuration

Local Security Policy
File Action View Help
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Defender Firewall with Advanced Security
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Computer
Advanced Audit Policy Configuration

Policy	Security Setting
Access Credential Manager as a trusted caller	
Access this computer from the network	Everyone,Administrators,Users,Backup Operators,System Managed Group,Device Owners
Act as part of the operating system	
Add workstations to domain	
Adjust memory quotas for a process	LOCAL SERVICE,NETWORK SERVICE,Administrators
Allow log on locally	Guest,Administrators,Users,Backup Operators,System Managed Group,Device Owners,Window Manager\Window Manager Group
Allow log on through Remote Desktop Services	Administrators,Remote Desktop Users
Back up files and directories	Administrators,Backup Operators
Bypass traverse checking	Everyone,LOCAL SERVICE,NETWORK SERVICE,Administrators,Users,Backup Operators,Device Owners
Change the system time	LOCAL SERVICE,Administrators
Change the time zone	LOCAL SERVICE,Administrators,Users,Device Owners

A separate user group with RDP access can be configured via local security policy settings. This group can be configured to allow remote access as a standard user, thus reducing risk if an account is compromised.

RELATED INFORMATION

- https://www.ic3.gov/media/2018/180927.aspx
- https://security.berkeley.edu/resources/best-practices-how-articles/system-application-security/securing-remote-desktop-rdp-system

Any additional questions or concerns can be sent to the Michigan Cyber Command Center (MC3) at mc3@michigan.gov or at 1-877-MI-CYBER

This document is the property of the Michigan Cyber Command Center (MC3) and is prepared for the limited purpose of information sharing. The information is designated UNCLASSIFIED/TLP WHITE. ***Information found within this document can be shared without restriction. This document must not be reclassified in any way, in whole or in part. Violation of this restriction will be cause from removal from MC3 distribution lists.***