MS-ISAC®
Multi-State Information Sharing & Analysis Center®

Intel Insight
December 2019 • IHT2019-1201

How to Disable Remote Desktop Protocol

Overview

The MS-ISAC observes specific malware variants consistently reaching The Top 10 Malware list. These specific malware variants have traits allowing them to be highly effective against State, Local, Tribal, and Territorial (SLTT) government networks, consistently infecting more systems than other types of malware. An examination of the characteristics of these malware variants revealed that they often abuse legitimate tools or parts of applications on a system or network. One such legitimate tool is Remote Desktop Protocol (RPD).

Understanding the Threat Surface

RDP is a Microsoft proprietary protocol that enables remote connections to other computers, typically over TCP port 3389. It provides network access for a remote user over an encrypted channel. Network administrators use RDP to diagnose issues, login to servers, and to perform other remote actions. Remote employees use RDP to log into the organization's network to access email and files.

Cyber threat actors (CTAs) use misconfigured RDP ports that are open to the Internet to gain network access. They are then in a position to potentially move laterally throughout a network, escalate privileges, access and exfiltrate sensitive information, harvest credentials, or deploy a wide variety of malware. This popular attack vector allows CTAs to maintain a low profile, as they are utilizing a legitimate network service that provides them with the same functionality as any other remote user. CTAs use tools, such as the Shodan search engine, to scan the Internet for open RDP ports and then use brute force password techniques to access vulnerable networks. Compromised RDP credentials are also widely available for sale on dark web marketplaces.

Recommendations

After evaluating your environment and conducting appropriate testing, use Group Policy to disable RDP. If RDP is needed for legitimate work functions, the MS-ISAC recommends following the below recommendations:

- Place any system with an open RDP port (3389) behind a firewall and require users to VPN in through the firewall.
- Enable strong passwords, multi-factor authentication, and account lockout policies to defend against brute-force attacks.
- Whitelist connections to specific trusted hosts.
- Restrict RDP logins to authorized non-administrator accounts, where possible. Adhere to the Principle of Least Privilege, ensuring that users have the minimum level of access required to accomplish their duties.
- Log and review RDP login attempts for anomalous activity and retain these logs for a minimum of 90 days. Ensure that only authorized users are accessing this service.
- Verify cloud environments adhere to best practices, as defined by the cloud service provider. After cloud environment setup is complete, ensure that RDP ports are not enabled unless required for a business purpose.

- Enable automatic Microsoft Updates to ensure that the latest versions of both the client and server software are running.
- Perform regular scans to ensure RDP remains externally closed to the Internet.

For additional help hardening your system, the MS-ISAC recommends organizations use the CIS Benchmarks and CIS Build Kits, which are a part of CIS SecureSuite.

Disabling RDP

The directions below are a general outline of how to disable RDP.

- Use **Group Policy setting** to Disable RDP:
  Click **Start Menu > Control Panel > System and Security > Administrative Tools.**
- Create or Edit **Group Policy Objects**.
- Expand **Computer Configuration > *Administrative Templates* > *Windows Components* > *Remote Desktop Services* > *Remote Desktop Session Host* > *Connections***.
- **Disable users from connecting remotely using Remote Desktop Services.**

For more information on how to enable or disable RDP please go to Microsoft.

The *MS-ISAC* is the focal point for cyber threat prevention, protection, response, and recovery for the nation's state, local, tribal, and territorial (SLTT) governments. More information about this topic, as well as 24x7 cybersecurity assistance is available at 866-787-4722, *SOC@cisecurity.org*. The MS-ISAC is interested in your comments - an anonymous feedback *survey* is available.