Public Service Announcement
FEDERAL BUREAU OF INVESTIGATION

27 September 2018

Alert Number
I-092718-PSA

Cyber Actors Increasingly Exploit The Remote Desktop Protocol to Conduct Malicious Activity

BACKGROUND

Remote administration tools, such as Remote Desktop Protocol (RDP), as an attack vector has been on the rise since mid-late 2016 with the rise of dark markets selling RDP Access. Malicious cyber actors have developed methods of identifying and exploiting vulnerable RDP sessions over the Internet to compromise identities, steal login credentials, and ransom other sensitive information. The Federal Bureau of Investigation (FBI) and Department of Homeland Security (DHS) recommend businesses and private citizens review and understand what remote accesses their networks allow and take steps to reduce the likelihood of compromise, which may include disabling RDP if it is not needed.

DEFINITION

Remote Desktop Protocol (RDP) is a proprietary network protocol that allows an individual to control the resources and data of a computer over the Internet. This protocol provides complete control over the desktop of a remote machine by transmitting input such as mouse movements and keystrokes and sending back a graphical user interface. In order for a remote desktop connection to be established, the local and remote machines need to authenticate via a username and password. Cyber actors can infiltrate the connection between the machines and inject malware or ransomware into the remote system. Attacks using the RDP protocol do not require user input, making intrusions difficult to detect.

VULNERABILITIES

- Weak passwords – passwords using dictionary words or do not include a mixture of uppercase/lowercase letters, numbers, and special characters – are vulnerable to brute-force attacks and dictionary attacks.

- Outdated versions of RDP may use flawed CredSSP, the encryption mechanism, thus enabling a potential man-in-the-middle attack.

- Allowing unrestricted access to the default RDP port (TCP 3389).

- Allowing unlimited login attempts to a user account.

EXAMPLES OF THREATS

CrySiS Ransomware: CrySIS ransomware primarily targets US businesses through open RDP ports, using both brute-force and dictionary attacks to gain unauthorized remote access. CrySiS then drops its ransomware onto the device and executes it. The threat actors demand payment in Bitcoin in exchange for a decryption key.

CryptON Ransomware: CryptON ransomware utilizes brute-force attacks to gain access to RDP sessions, then allows a threat actor to manually execute malicious programs on the compromised machine. Cyber actors typically request Bitcoin in exchange for decryption directions.

Samsam Ransomware: Samsam ransomware uses a wide range of exploits, including ones attacking RDP-enabled machines, to perform brute-force attacks. In July 2018, Samsam threat actors used a brute-force attack on RDP login credentials to infiltrate a healthcare company. The ransomware was able to encrypt thousands of machines before detection.

Dark Web Exchange: Threat actors buy and sell stolen RDP login credentials on the Dark Web. The value of credentials is determined by the location of the compromised machine, software utilized in the session, and any additional attributes that increase the usability of the stolen resources.

SUGGESTIONS FOR PROTECTION

The use of RDP creates risk. Because RDP has the ability to remotely control a system entirely, usage should be closely regulated, monitored, and controlled. The FBI and DHS recommend implementing the following best practices to protect against RDP-based attacks:

- Audit your network for systems using RDP for remote communication. Disable the service if unneeded or install available patches. Users may need to work with their technology vendors to confirm that patches will not affect system processes.

- Verify all cloud-based virtual machine instances with a public IP do not have open RDP ports, specifically port 3389, unless there is a valid business reason to do so. Place any system with an open RDP port behind a firewall and require users to use a Virtual Private Network (VPN) to access it through the firewall.

- Enable strong passwords and account lockout policies to defend against brute-force attacks.

- Apply two-factor authentication, where possible.

- Apply system and software updates regularly.

- Maintain a good back-up strategy.

- Enable logging and ensure logging mechanisms capture RDP logins. Keep logs for a minimum of 90 days and review them regularly to detect intrusion attempts.

- When creating cloud-based virtual machines, adhere to the cloud provider's best practices for remote access.

- Ensure third parties that require RDP access are required to follow internal policies on remote access.

- Minimize network exposure for all control system devices. Where possible, critical devices should not have RDP enabled.

- Regulate and limit external to internal RDP connections. When external access to internal resources is required, use secure methods, such as VPNs, recognizing VPNs are only as secure as the connected devices.