Ransomware: The many dangers of Remote Desktop Protocol

In the first part of this series, we gave a basic overview of ransomware and how it works. Now, we are delving deeper into the specific ways in which ransomware operators infiltrate your systems, starting with Remote Desktop Protocol.

Due to the pandemic, the proportion of people working from home has more than doubled. It is a trend that shows no sign of abating; more than half (54%) of **employees say they would prefer to continue working from home even when restrictions fully end**.

Unfortunately, while it has become a necessity during the pandemic, employees working remotely and using remote access tools like **Remote Desktop Protocol (RDP)** to access company data are at high risk. Between May and August in 2021, ESET detected 55 billion new brute-force attacks against networks with public-facing RDP services. This was up 104% compared to the period from January to April, and up sixfold when comparing H1 2020 to H1 2021.

RDP's rising popularity

RDP has been included with every version of Microsoft Windows from Windows XP onward. However, its popularity rose substantially during the pandemic as a way for staff forced to work from home to access company servers remotely via their laptops, phones and tablets. While it has undoubtably been useful to allow remote access to corporate systems, **RDP has become open to abuse by those with criminal intentions** because:

- Vulnerable RDP systems are easy to find
- It is easy for attackers to obtain a foothold on RDP systems to plant ransomware if they have poor configuration
- Many RDP systems have weak configuration and attackers can exploit the default RDP port 3389, which is commonly used for connection
- Tools and techniques for escalating privilege and obtaining admin rights on compromised RDP systems are widely known and available

A twofold responsibility

The rise in ransomware attacks seen via RDP demonstrates how critical robust security practices are when configuring and using collaboration tools and other business systems. Remember that security is a twofold responsibility within the business, **first for the IT admins who set the rules and monitor activity, and second for all staff who use the tools**. Whether they like it or not, all staff – from consultants to the CEO – who use tools such as RDP to undertake their work remotely have signed up for a role in securing their environment. It is not something to take lightly.

To defend systems running RDP against unauthorized access, businesses should:

- Have policies in place to address remote access security, such as requiring RDP to only be accessed over a VPN (virtual private network) or with the use of MFA (multifactor authentication)
- Make sure everyone is complying with the rules, while also being prepared for the possibility of an attack succeeding despite these rules
- Not allow staff to connect the server running RDP to both the organization's network and the internet until it is securely configured
- Make an inventory of all internet-facing assets and decide which need remote access. If access really is necessary, require long passwords and insist upon access only from a secure VPN
- Harden and patch all remotely accessible devices. Make sure that all nonessential services and components have been removed or disabled, and that settings are configured for maximum security

Layers of protection are required

RDP has become a critical component of today's hybrid workplace. However, it has provided a pathway for bad guys wanting to infiltrate corporate systems and implant ransomware. Deep-reaching IT admin skills, enhanced system settings and an improved security culture are all critical to addressing the security demands brought by both hybrid work and the large uptick in collaboration and productivity platforms such as RDP.

All of this needs to be underpinned by robust, award-winning cybersecurity solutions that protect your company endpoints, data and users.