Trusted Cyber Technologies

THALES
Building a future we can all trust

How Ransomware attacks leverage unprotected RDPs and what you can do about it

Ransomware attacks targeting enterprises in a variety of sectors have skyrocketed during the first half of 2020. Criminals are taking advantage of our reliance on digital communications and remote working for sinister purposes. As a result, most of the ransomware incidents can be attributed to a limited number of intrusion vectors, with the top three being badly secured remote desktop protocol (RDP) endpoints, email phishing, and the exploitation of zero-day VPN vulnerabilities.

Reports from Coveware, Emsisoft, and Recorded Future highlight that "RDP is regarded as the single biggest attack vector for ransomware" and the source of most ransomware incidents in 2020. Some might think that RDP is the top intrusion vector for ransomware because of the current work-from-home setups. However, this is not correct. RDP has been among the top intrusion vectors since last year when ransomware attackers stopped targeting consumers and took aim at companies and critical infrastructure instead.

What is the root cause?

RDP is the most popular technology for connecting to remote systems, and is generally regarded as a safe and secure tool when used within a private network. However, when RDP ports are left open on the internet and accessible with simple passwords, they can cause serious security problems. Passwords can be easily compromised paving the way for malicious and unauthorized access to corporate networks via unprotected RDPs. Unauthorized access via RDPs allows attackers to gain access to organizational servers and act as a launch pad for ransomware attacks.
There are millions of computers with their RDP ports exposed online without any protection, which makes RDP a huge attack vector to all sorts of malicious cyber activities, and increasingly ransomware attacks. Criminals seeking to exploit these access points can find them for free on "RDP markets". From there on, their job is business as usual. They look for weak passwords leveraging well-known techniques like brute force or social engineering. Once the attacker has gained access to the target system, they focus on making the network as insecure as possible.

After security systems have been disabled and the network is left unprotected, the criminals are free to deliver their malicious package. This might be anything from installing ransomware, deploying keyloggers, using compromised machines to distribute spam, stealing sensitive data, or installing backdoors for future attacks.

Best practices to mitigate RDP attacks

As mentioned above, RDPs are access points to get inside an organization's networks and should not be seen on the internet or published unprotected. Publishing remote desktops for user convenience does not justify the increased threat organizations are exposed to.

For organizations that require RDP, the following best practices focus on hardening the access point and are useful for securing RDP against brute force attacks.

- As a rule, do not publish unprotected remote desktops on the internet. If this is an absolute necessity, make sure the RDP access point is protected with multi-factor authentication (MFA) to ensure that only validated users can enter the RDP.
- Use RDP gateways. Remote desktops should be protected behind reverse proxy gateways to obfuscate the standard RDP port 3389. RDP gateways are accessed over HTTPS connections (port 443) protected through the TLS encryption protocol.
- Apply MFA to access the RDP gateway. Even the strongest passwords can be compromised. While not a panacea, MFA offers an extra layer of protection by requiring users to provide at least two forms of authentication to log into an RDP session.
- Apply MFA to the network logon. Once inside the remote desktop, implement another layer of security by applying MFA to the network logon point.

How Thales SafeNet Trusted Access Helps Mitigate Attacks

Thales SafeNet Trusted Access can help you protect your organization's environment against RDP-based ransomware attacks. SafeNet Trusted Access allows organizations to effectively secure remote access to RDPs, RDP gateways as well as additional cloud and legacy apps, regardless of the end-point device being used. SafeNet Trusted Access offers:

- Support for a broad range of authentication options including adaptive and step up authentication, MFA and hardware-based tokens
- Flexible access policies for all OS (Windows/Mac/Linux) - this means you can use a single access management and authentication service to protect cloud based apps and all remote desktops, regardless of which OS they run.
- Centrally manage cloud apps and network logons from a single Access Management/MFA service.

SafeNet Trusted Access is available for sale to the U.S. Federal Government exclusively through Thales Trusted Cyber Technologies.

About Thales Trusted Cyber Technologies

Thales Trusted Cyber Technologies, a business area of Thales Defense & Security, Inc., protects the most vital data from the core to the cloud to the field. We serve as a trusted, U.S. based source for cyber security solutions for the U.S. Federal Government. Our solutions enable agencies to deploy a holistic data protection ecosystem where data and cryptographic keys are secured and managed, and access and distribution are controlled. For more information, visit www.thalestct.com

3465 Box Hill Corporate Center Drive, Suite D, Abingdon, MD 21009 • 443-484-7070 • info@thalestct.com
thalestct.com