#1 Choice of DIGITAL WORLD

eScan™
Enterprise Security

Blocking RDP hacking attacks with eScan TSPM Technology

eScan Launches new TSPM Technology to block RDP hacking attacks

With the growing complexity of cyber-attacks, enterprises are spending millions to avoid cyber-crime. However, due to bad security practices such as usage of elementary passwords for system access creates most vulnerable opportunity for cyber criminals. In such scenarios cyber criminals use brute force attack to take control of network. Based on "National Exposure Index" report by Rapid7, 73% of Indian RDP servers are exposed to bruteforce attacks, and ranks 18th on the Global Index.

In the last 2 months, eScan has noted that most ransomware attacks could be contributed to cyber criminals using rogue RDP sessions to take control of servers & injecting ransomware in order to extort ransom from unsuspecting companies. The methodology to do this is being smartly executed by taking all possible steps to pro-actively disable real-time monitoring technology and/or uninstalling any anti-malware products installed on the said end-points.

IT Administration and management of assets for every Organization is a tedious task, and in order to simplify this process of troubleshooting / maintenance, IT Administrators make use of various Remote Access Technologies viz. Remote Desktop Protocol (RDP) so as to access the graphical interface of another computer over a network connection.

It is to be noted that the security of RDP is limited to strong passwords and a secure connection by way of implementing TLS so as to mitigate various forms of brute-force / password guessing attacks or MITM attacks.

Due to various reasons not every organization implements password policies, and in many cases it is the user who has to choose their own password. Furthermore, password reuse is another area of concern which has to be addressed.

Usage of RDP

To facilitate Centralized Management of computers, organizations implement RDP and access these systems either through LAN or Internet. In order to protect RDP enabled systems from outsiders, VPN might be implemented but in majority of cases, Administrators configure the firewall to open up RDP for the systems they would want to manage remotely.

RDP Attacks

Pen-testing platforms such as Kali offer RDP Bruteforce and Exploit tools which are being specifically used for targeting systems with Internet facing RDP systems. Bruteforce attack would generate large numbers of Failed Login Notifications and are logged. Furthermore, the users are not even aware of the on-going Brute Force attack, since it is not imperative that the attack would take place when the user would be logged in and working on the system.

- Failed RDP Authentications although are subjected to Log Audits, but users are never alerted whenever they succeed in breaching the security. This has resulted in the rise of Brute Force of RDP sessions.
- Due to the fact that users were never aware of the on-going RDP authentications, the perpetrators in all the cases were able to gain complete control of the system.
- Attackers upon successful exploitation would implement backdoors or pivot to other systems and in some cases infect the systems with Ransomware.

TSPM – Terminal Services Protection Module

eScan's Terminal Services Protection Module (TSPM) not just detects these brute force attempts but also heuristically identifies suspicious IP Addresses / Hosts and blocks any access attempts from them and in order to safeguard the systems from future attacks, the IP addresses and Hosts from future attacks are banned from initiating any further connections to the system.

As mentioned earlier, it has been known that attackers would try to uninstall security applications from compromised systems in order to cover up their tracks and stop the administrators from getting alerted about the breach. eScan TSPM detects and stops these attempts too, moreover the administrators are also alerted about the preventive measures initiated by TSPM.

In the present landscape where attackers are trying to exploit every known weakness be it unpatched systems or inability of the users / administrators to maintain password hygiene, eScan's TSPM would protect the systems/organizations from such attacks.