RDP Monitor Plus Debuts to Safeguard Remote Desktop Activity from Increasing Onslaught of Malware and Ransomware Attacks

RDP Monitor Plus allows admins to monitor RDP attacks in real-time via its no-cost license.

OCEANSIDE, CALIFORNIA, UNITED STATES, June 18, 2020 /EINPresswire.com/ -- RDP Monitor Plus is a brand-new product helping to solve an age-old computing concern of protecting remote access to Windows Servers from attacks outside of corporate networks. The groundswell of added 'work from home' remote users accessing cloud-based corporate networks has led to a corresponding increase in Remote Desktop Protocol (RDP) technology usage, which has unfortunately brought about a dramatic spike in malware and ransomware attacks. Victims of these attacks include small, medium and large organizations in various industries.

Access via RDP is secured by a simple username and password combination. Therefore, remote attackers can attempt brute force tactics to gain access to corporate machines and networks. The attacks number in the millions of attempts and are rising sharply. Due to a lack of monitoring and mitigation, attacks are unfortunately all too often successful. Once an attacker has breached a machine, they can sell the credentials to the highest bidder, install malware, potentially access other machines on your network, and utilize ransomware to hold a machine or network hostage. In fact, RDP is the most common attack vector for ransomware attacks with more than 50% of compromised machines being traced directly to RDP (Coveware, 2020).

Network Administrators and CIO's need to provide flexible remote access to their workforce while maintaining a focus on the overall security of their network. RDP Monitor Plus allows admins to monitor RDP attacks in real-time via its no-cost license. IP addresses and nation-of-origination are unveiled, which allow you to measure the breadth and depth of the attacks. The paid license to RDP Monitor Plus allows for always-on IP blocking when attacks eclipse certain levels such as multiple attempts per second or attacks that number dozens or hundreds of failed consecutive attacks over a longer duration. RDP Monitor Plus therefore assists organizations to both monitor and thwart brute force attacks on their environment.

RDP Monitor Plus runs as a Windows service so that it can protect the machine even if there is no user actively logged-on. The paid version's monitoring algorithms detect attacks that meet certain criteria. Offending source IP's can then be automatically blocked via the Windows

Firewall. Known ‘safe’ users can of course be whitelisted, and blocked IP addresses can also be released after a set period of time. The ability to block attackers by specific IP addresses allows for a dramatic decrease in overall brute force attacks on the machine and thereby decreases the likelihood that the attacks circumvent existing security.

PRICING, DOWNLOAD, AND CORPORATE INFORMATION
The no-cost version of RDP Monitor Plus can be downloaded and used immediately. The RDP Monitor Plus paid version is offered on a per-machine per-year license of $99. You may find the product download at: https://www.guardports.com. RDP Monitor Plus is a product of TrustyMug LLC, a California corporation. TrustyMug specializes in cloud-based technologies that secure and empower computing in the modern world.

Gregory Wietholter
TrustyMug
+1 619-800-8066
email us here
Visit us on social media:
Twitter
