Malwarebytes

SOLUTION BRIEF

Brute Force Protection

Reduce your exposure to malware delivery via compromised RDP connections

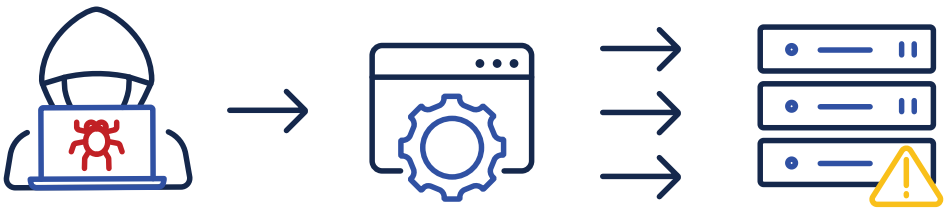
What is a brute force attack?

A brute force attack is a malicious tactic that relies on guessing possible combinations of passwords until the correct password is discovered. If successful, the attack can be used to deliver various types of malware that may decrypt encrypted data and spread laterally throughout a network.

Overview

The massive transition to work from home caused a proportionate increase in remote desktop protocol (RDP) connections. Increasingly, IT professionals are using RDP to assist their remote workforce, and at home, workers are using RDP to access workstations and file servers in their offices. The rise of RDP connections is also unfortunately correlated to the influx of brute force attacks by cybercriminals. In fact, **between March and April 2020, brute force attacks increased from 200k to over 1.2M per day in the United States** according to BleepingComputer.

Brute force attacks are simple and reliable. Once a cybercriminal discovers the correct password to an available RDP connection, they can gain access to the endpoint and deposit any type of malware to infect the endpoint and spread laterally throughout the network. **Brute force attacks are becoming an extremely common means of spreading ransomware**, which often demands high payments and causes long periods of downtime.



KEY BENEFITS

An additional level of protection to stop brute force RDP attacks before they compromise servers and workstations.

Simple configuration management via the cloud-based Nebula console.

Fully automated brute force protection offers around-the-clock security.

Instant alerts and notifications when a brute force attack occurs.

Superior protection against brute force attacks

The Brute Force Protection feature offered by Malwarebytes reduces vulnerabilities of RDP connections. By tracking repeated failed login attempts, Malwarebytes can selectively block malicious Host IPs, preventing the cybercriminal from successfully completing a brute force attack and infecting endpoints with malware payloads.

Brute Force Protection is built for both servers and workstations. Native to the Nebula cloud platform, this feature alerts security teams whenever malicious activity occurs over RDP connections. The configuration of the brute force protection feature is simple and intuitive within the Nebula console.

Benefits of Brute Force Protection

An additional level of protection helps stop brute force attacks of RDP connections before they compromise servers and workstations. Network breaches can lead to ransomware infections, phishing email campaigns, and other cyberattacks.

Simple management via the cloud-based Malwarebytes Nebula console offers a single pane of glass view of endpoints across your distributed network. Full visibility allows your team to act quickly when malicious activities occur.

Fully automated Brute Force Protection never sleeps – it works silently and seamlessly in the background to protect RDP connections without any end-user interaction.

Never miss a beat with a solution that automatically alerts your team whenever an attempted brute force attack occurs.

Highly effective, yet lightweight, Brute Force Protection has been designed to be extremely resource efficient while providing strong protection of RDP connections.

Stop brute force attacks on RDP connections

Brute force attacks on RDP connections are part of the remote work "new normal." Cybercriminals are heavily targeting RDP password vulnerabilities to deposit malware, such as ransomware and spyware. The Brute Force Protection feature minimizes RDP connection exposure and blocks attacks as they happen.

LEARN MORE

Visit www.malwarebytes.com/business/cloud to learn about the Brute Force Protection feature.

malwarebytes.com/business corporate-sales@malwarebytes.com 1.800.520.2796

Malwarebytes is a cybersecurity company that millions worldwide trust. Malwarebytes proactively protects people and businesses against malicious threats, including ransomware, that traditional antivirus solutions miss. The company's flagship product uses signature-less technologies to detect and stop a cyberattack before damage occurs. Learn more at www.malwarebytes.com.