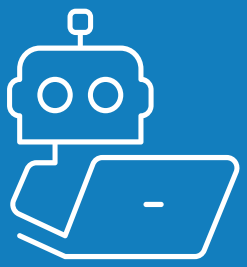
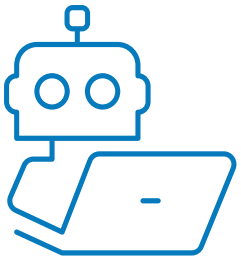
PREBYTES



Remote Desktop Detection

Identification of threats related to the use of sharing desktop software

prebytes.com



Remote Desktop Detection identifies the presence of remote desktop software while using the online service.

This innovative solution is a response to the growing popularity of the remote desktop attack method among cybercriminals. A common technique used by cybercriminals is to impersonate an organization during a phone call (vishing). Cybercriminals attack clients through manipulation and exploitation of their inexperience. Users are often unaware that sharing their desktop enables criminals to access confidential data, banking, or other services, thus account takeover (ATO).

Remote Desktop Detection allows to detect of unauthorized hijacking of a device and determine session security. It has multiple anomaly detection mechanisms; active and passive, which work together to ensure remote desktop detection efficiency.

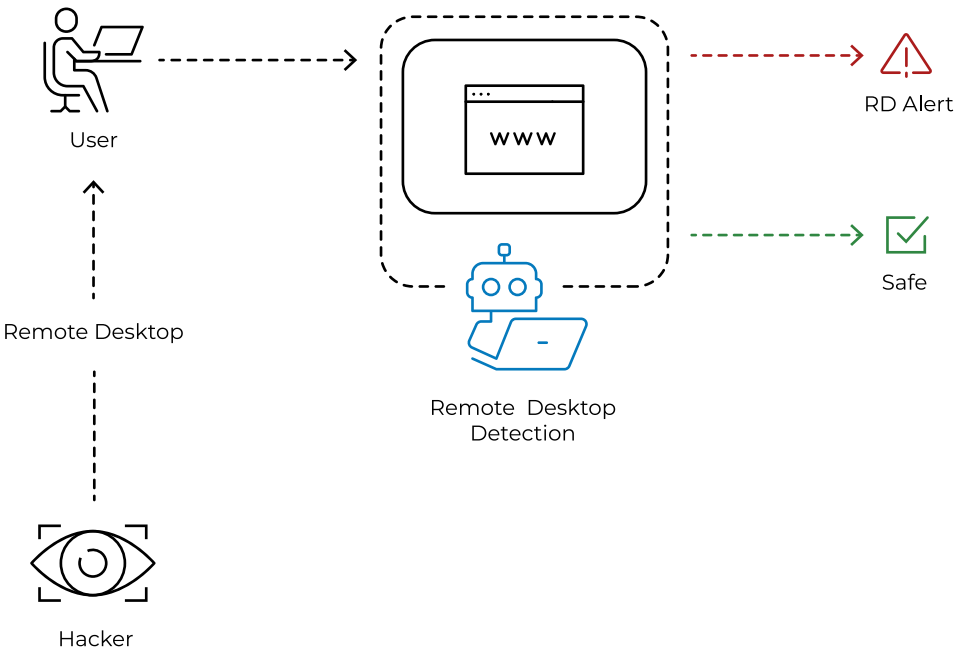
Active detection analyses device configuration and provides real-time diagnostics. It recognizes many commonly used desktop sharing applications and determines which application is in use at the time.

Passive detection is a behavioral analysis using an intelligent algorithm developed using artificial intelligence and then optimized to detect deviations from typical user behavior instantly.

A passive mechanism allows you to diagnose the takeover of the device in real-time.

PREBYTES sustains the process of protecting the service and the user through regular tests. As a part of the detection improvement process, the specialist team simulates attacks using real devices.

Remote Desktop Detection diagram



Remote Desktop Detection can be delivered as a module of the MPShield Security As a Service or a ready-to-use, stand-alone solution implemented in any online service.

Remote Desktop Detection summary:

- You can detect the presence of remote desktop software on the user's device.
- You can guarantee the protection of online service users against cybercriminals attacks.
- You will detect the exact time when cybercriminals take active control over the user's device.
- You will minimize the risk of losing users' funds and trust.
- You will limit the leakage of confidential information. The confidence and sense of security of the service users will rapidly improve.
- You will save time and resources lost in handling fraud claims.

6 Sandomierska Street
37-300 Leżajsk
Poland

sales@prebytes.com
+48 537 337 551
prebytes.com