PRIXL

PRIXL RESEARCH · WHITEPAPER

Remote Desktop Under Attack

Six months of password attacks on the servers of Indian CA firms, and what stopped them

Edition 1 · October 2026 · Prixl Technologies

Summary

Between late March and early October 2026, Prixl Warden recorded every failed sign-in on the Windows servers of three chartered accountant firms in India. In that time the three servers received **3.9 million password attempts from the internet**, from 9,052 different addresses.

3.9 million
password attempts from the internet against three CA firm servers in six months

1 in 4
of those attempts came from addresses in India

62%
of attempts tried the username "administrator"

99.97%
fewer attempts reached the server once Remote Desktop was closed to the internet

Five findings matter most for a small firm:

1. **The attacks are constant and automated.** On its busiest day one server received 143,259 attempts, almost two every second. Attempts arrive at the same rate at 3 am as at 3 pm.
2. **A quarter of the attacks come from inside India.** Blocking foreign countries would leave the largest single source untouched.
3. **Attackers know their audience.** After "administrator" and "admin", the list includes "accounts", "tally" and nine other Tally-style names, tried from 113 different addresses.
4. **Closing Remote Desktop to the internet works.** On the one server we watched before and after the change, attempts that reached Windows fell from about 25,500 a day to 8.
5. **A switched-off firewall reopens what you closed.** When one server's firewall was switched off for five days, the first attack arrived about half an hour later and more than 370,000 followed.

1. What we measured

Prixl Warden is an agent that runs on a firm's Windows server. Among other things, it reads the Windows security log and reports every failed sign-in, with the address it came from and the username it tried, to Prixl's cloud.

This paper uses those reports from **three servers at three CA firms in India**, from late March to early October 2026. It also uses cloud test servers that Prixl runs on the internet, which show what a brand-new server faces. One firm server has a four-week gap in its records.

We count an **attack attempt** as a failed sign-in from a public internet address. Failed sign-ins from inside the office network (308,098 of them, mostly mistyped or saved passwords) are left out.

Three servers is a small sample, and we say so throughout. The attack-side numbers (addresses, countries, usernames, timing) rest on millions of events and are robust. Statements about the firms themselves are observations of three servers, not rates for the profession. Nothing in this paper identifies a firm, a server, a person or an IP address: servers are not labelled, single-firm events carry no dates, and no username of a real account is shown.

2. The volume

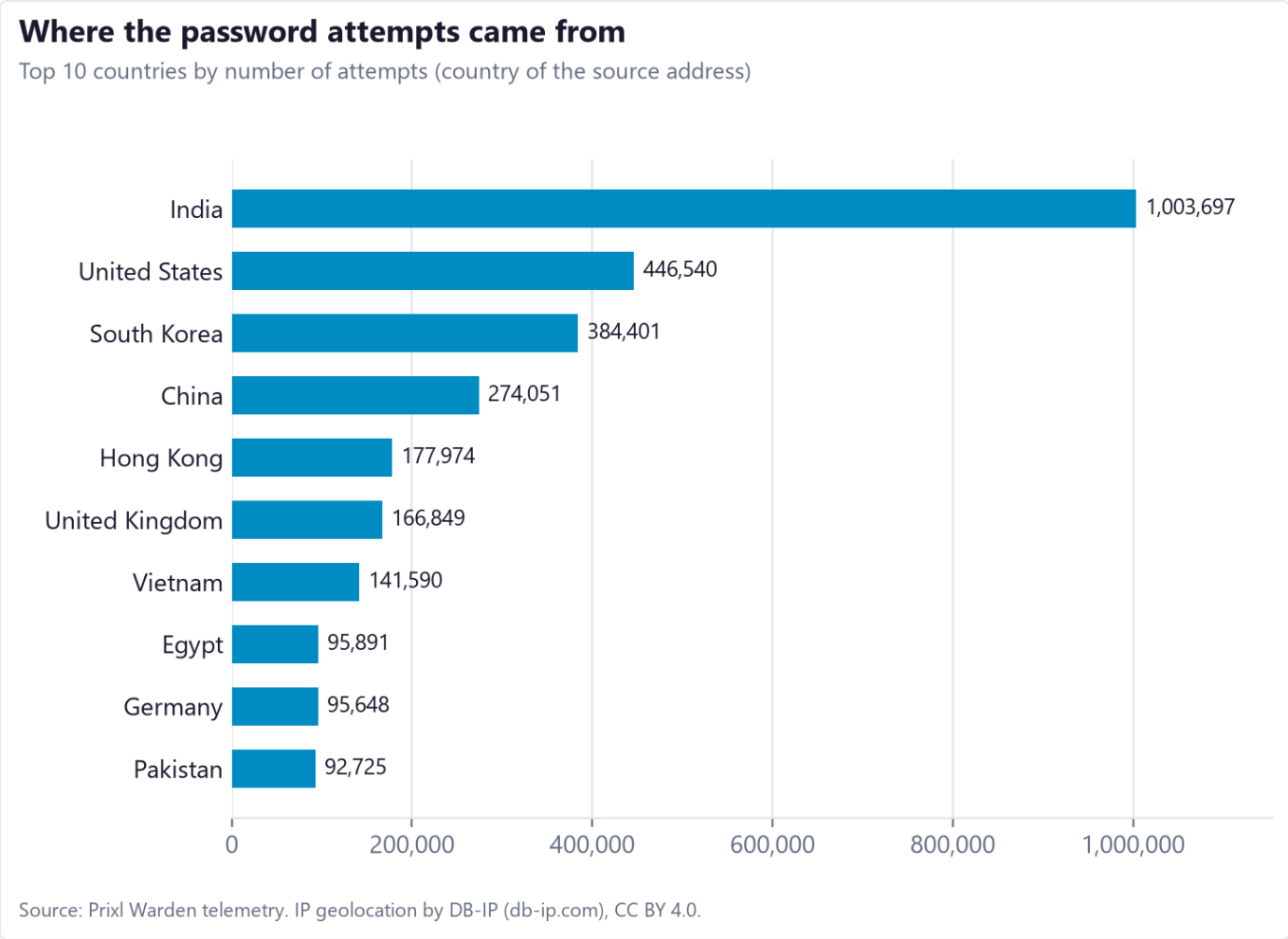
Two of the three servers were under continuous attack while Remote Desktop was reachable from the internet, at roughly **25,000 to 30,000 attempts a day each**. The busiest single day brought 143,259 attempts to one server. The third server received 237 attempts in six months, all on one day.

Nearly every attempt (99.99%) arrived as a "network" sign-in: the type Windows records when credentials are checked over the network, which includes Remote Desktop with Network Level Authentication, the setting Microsoft recommends. That kept these attempts at the door. It did not make them stop.

A new server is found in minutes

To see how quickly an unknown server is found, we watched one of Prixl's own cloud test servers from the moment its monitoring started. **The first password attempt arrived 1 minute 52 seconds later.** Over the next three days it received 3,111 attempts. Nobody needs to know a server exists for it to be attacked: automated scanners try every address on the internet.

3. Who is knocking



Country of the source address. IP Geolocation by DB-IP, licensed CC BY 4.0.

Including those on our cloud test server, the attempts came from **9,071 addresses in 142 countries**. India was the largest source by a wide margin: **1,003,697 attempts, 25.7% of the total**, from 1,490 addresses. By number of addresses, China was first (1,634), then India and the United States.

This matters because a common first reaction is to block foreign countries. In our data that would have left the largest single source untouched, and every address can be swapped for another in seconds.

A few addresses do most of the work. The busiest 1% of addresses sent 52% of all attempts. Half of all addresses tried six times or fewer, and 58% were seen on one day only. Attacks come from a constantly changing crowd, with a small core of persistent ones: 861 addresses came back on seven or more different days.

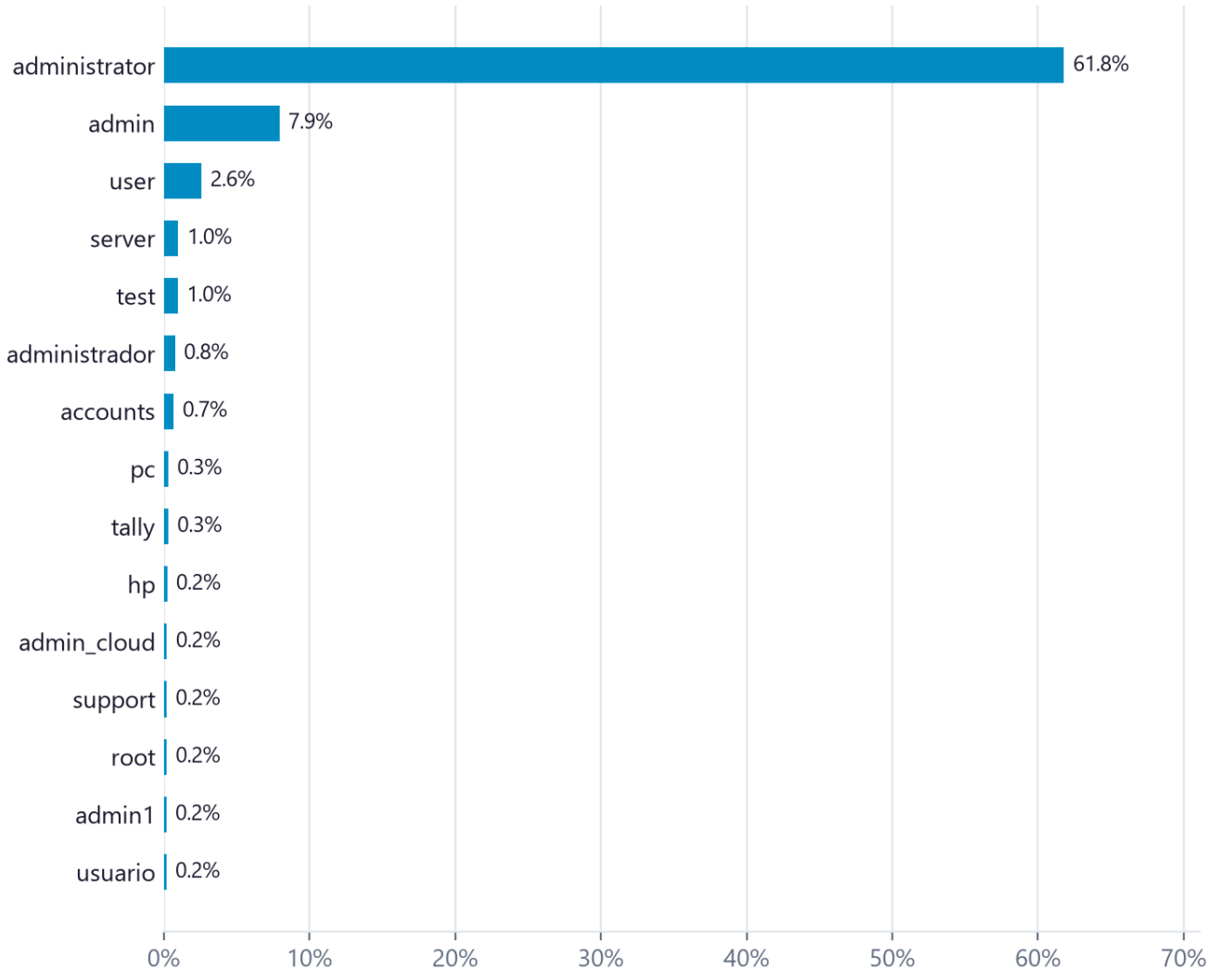
Many attackers hit more than one firm. One in five attacking addresses (1,859) tried more than one of the three firms. These are not targeted attacks on a particular firm. They are the same automated tools working through every server they can find.

Most of the addresses belong to hosting and cloud networks. The networks with the most attacking addresses were large Chinese telecom carriers and cloud platforms, international cloud and hosting companies, Indian hosting providers, and Indian mobile networks. That tells you where the traffic came from, not who was behind it: rented and hijacked machines are the usual tools, and the providers are not the attackers, so we do not name them.

4. What they try

The usernames attackers try

Share of internet password attempts, top 15 names (each tried from at least 5 addresses)



Source: Prixl Warden telemetry.

Only names tried from at least five different addresses are shown, and never a name that belongs to a real account on a monitored server.

Attackers tried **49,548 different usernames**. Most attempts went at a handful:

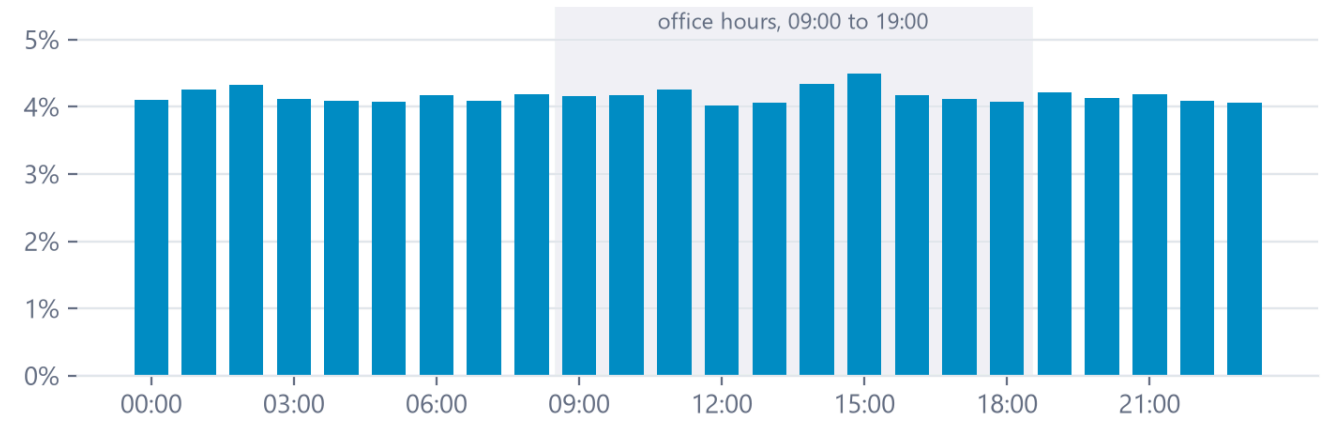
- **"administrator": 61.8%** of all attempts. Together with "admin", "administrador" and "administrateur", the administrator family took **70.7%**.
- Generic names follow, such as "user", "server", "test", "pc", "support" and "backup".
- **Names aimed at accounting offices.** "accounts" (26,522 attempts), "finance", "audit", "accountant", and ten names built on **"tally"** (19,741 attempts from 113 addresses). Someone has added India's most popular accounting software to their word lists.
- 0.85% of attempts used an empty username.

Two lessons follow. The built-in Administrator account is the target of most attacks, so it should not be the account anyone signs in with: rename or disable it, and give each administrator a named account. And an account named after a role or a software product, such as "accounts" or "tally", is a guessable target too.

5. When they come

Attacks do not keep office hours

Share of internet password attempts by hour of day, Indian Standard Time



Source: Prixl Warden telemetry, three customer servers and two cloud test servers.

Every hour of the day carried between 4.0% and 4.5% of all attempts. **Two-thirds of attempts (65.5%) arrived outside office hours**, which is almost exactly what you would expect if attacks ignore the clock altogether, because most hours of the week are outside office hours.

The practical point: nobody is watching the server when most attacks happen. Monitoring has to work without a person at the screen, and alerts have to reach someone's phone.

6. What made the difference

Closing Remote Desktop to the internet

One server was reachable on Remote Desktop from the internet until the firm restricted who could reach it. The change is visible in the record:

Period	Attempts reaching Windows, per day
Before the change (reachable)	25,527
After the change (closed)	8

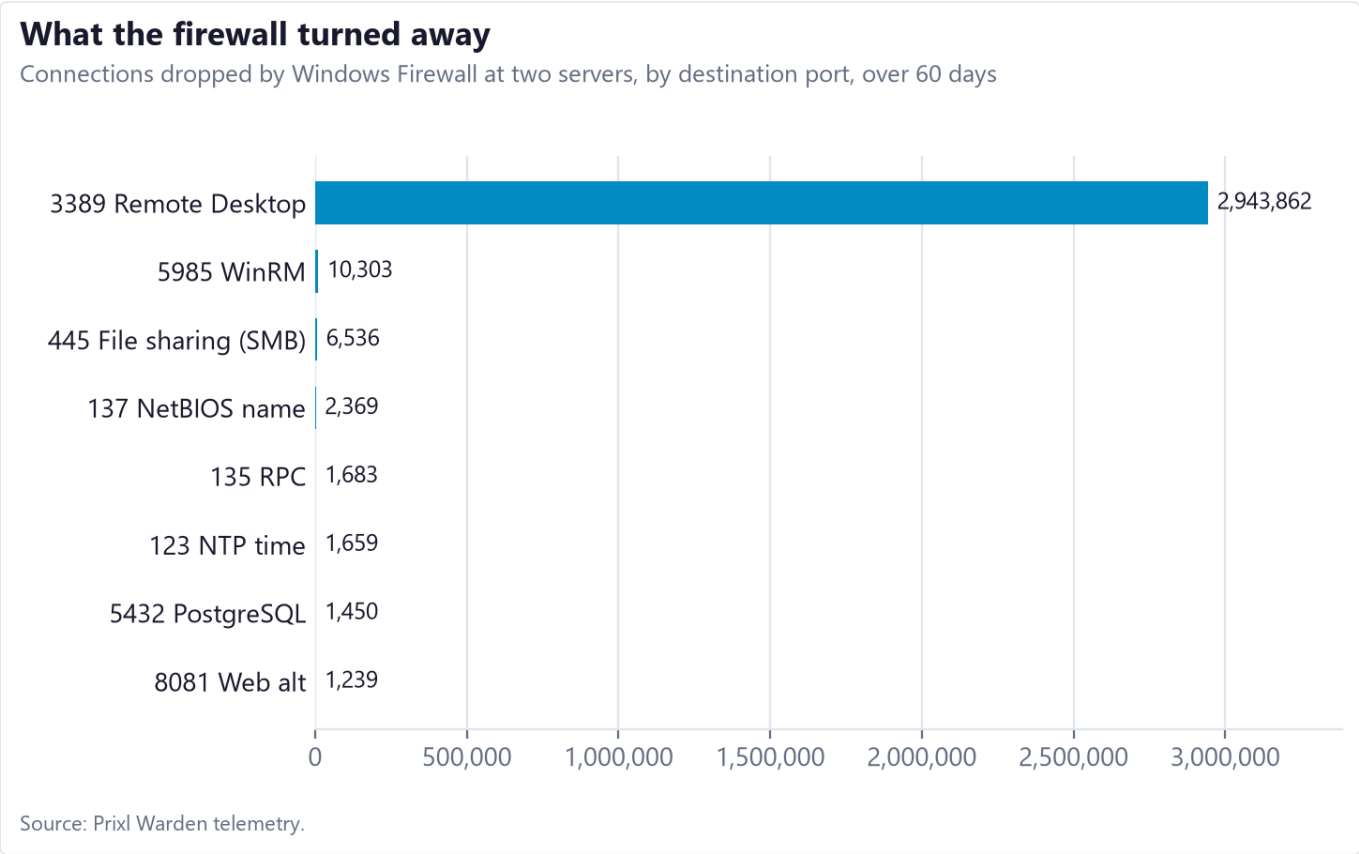
Attempts that reached Windows fell by 99.97%. The scanning did not stop: Windows Firewall on that server still turned away an average of **8,023 connections a day**, almost all of them on the Remote Desktop port. The difference is that none of them reached the sign-in screen.

A second server shows a similar fall later in the year: from 30,257 attempts a day to **117 a day**, while its firewall turned away an average of 43,242 connections a day on the same port. We have not tied that change to a single recorded action, so we report the numbers without a cause.

Automatic blocking

Prixl Warden can add a firewall rule that blocks an address after repeated failures. Leaving aside the incident in Section 7, which on its own accounts for most block rules, it added 4,602 block rules for 2,373 addresses between July and October. **A third of blocked addresses (33%) came back** and were blocked again after their block expired. Blocking takes away the noise and the most persistent attackers, but it is a second line of defence: with Remote Desktop open, each new address still gets its first guesses.

What the firewall turned away



Over the 60 days for which firewall logs are available, the two servers' firewalls dropped **2,976,477 connections. 98.9% were aimed at Remote Desktop (port 3389).** Next came WinRM (5985), Windows' remote management service, and file sharing (445). Remote Desktop is overwhelmingly what attackers look for on a Windows server, so it is the first thing to close.

7. When the firewall was switched off

Minutes after new software was installed on the first server, **its Windows Firewall was switched off.** It stayed off for almost five days. With the firewall off, Remote Desktop was once again reachable from the internet.

- **The first attack arrived about half an hour later.**

- In under five days the server received **more than 370,000 password attempts** from about 250 addresses, around **75,000 a day**: nearly three times its rate before Remote Desktop was closed.
- Prixl Warden kept adding block rules, about 190,000 of them, but **a firewall rule does nothing while the firewall is off.**
- Once the firewall was back on, attempts fell straight back to a handful a day.

At the time, Prixl Warden did not yet watch for a switched-off firewall. It now alerts immediately when a firewall profile is switched off. The wider lesson does not depend on any product: a single software installation can reopen everything you closed. Another of the three servers had at least one firewall profile switched off in every one of its 38 audits from March to October. Check that all three firewall profiles are on after installing any software, and use monitoring that tells you when they are not.

8. What a firm should do

1. **Close Remote Desktop to the internet.** Reach the server through a VPN and allow Remote Desktop only from it. On the server we watched, it cut the password attempts reaching the server by 99.97%; the scanning continued at the firewall.
2. **Keep Windows Firewall on for all three profiles,** and check it after installing any software, especially remote-support tools. Better, be alerted automatically when a profile is switched off. Two of the three servers had a profile switched off during the study.
3. **Do not use the built-in Administrator account.** Rename or disable it, and give each administrator a named account with a long passphrase.
4. **Avoid guessable account names** such as "accounts", "tally" or "admin".
5. **Turn on account lockout** (5 to 10 attempts, at least 15 minutes, and "Allow Administrator account lockout" on older servers) and **block addresses that keep failing.**
6. **Do not rely on country blocking.** A quarter of the attacks came from India.
7. **Make alerts reach a person.** Two-thirds of attacks arrive when nobody is in the office.
8. **Remember CERT-In.** If an attacker does get in, the 2022 directions give you six hours from noticing to report it. Prepare before you need to.

Method and limits

Data. Failed sign-ins (Windows event 4625) recorded by Prixl Warden, including events the agent combined into a single record with a repeat count. Firewall drops come from the Windows Firewall log, available for the last 60 days of the period. Block rules come from Warden's own records for the last three months. Times are Indian Standard Time.

Scope. Three customer servers at three CA firms, plus Prixl's cloud test servers where stated. One server has a four-week gap in its records, and its per-day rates use only days with data.

Countries and networks. Countries are those of the source address in the DB-IP Lite database (October 2026, CC BY 4.0). Network types are from iptoasn.com. A country or network tells you where traffic came from, not who sent it.

Privacy. Only aggregates are published, under section 8 of the Prixl Warden licence terms. Usernames are shown only if at least five different addresses tried them and the name never belonged to an account that signed in successfully, except the Windows built-in names "administrator", "admin" and "guest". No firm, person, address, network operator or server is identified.

PRIXL

About Prixl. Prixl Technologies builds Prixl Warden, which watches and hardens the Windows servers of small professional firms and alerts the partners when something needs attention, and Prixl Guard for private remote access. Free resources, including an Information Security Policy template for CA firms, are at prixl.io. Questions: support@prixl.io.

General information about attacks we observed, not legal or professional advice. © 2026 Prixl Technologies. You may share this paper in full, unchanged, with credit to Prixl Technologies. Charts and figures may be quoted with the credit "Source: Prixl Technologies, Remote Desktop Under Attack, October 2026".