Endpoint | 4 MIN READ NEWS

List of Common Passwords Accounts for Nearly All Cyberattacks

Half of a million passwords from the RockYou2021 list account for 99.997% of all credential attacks against a variety of honeypots, suggesting attackers are just taking the easy road.

Robert Lemos
Contributing Writer, Dark Reading

October 21, 2022

Source: Brian Jackson via Alamy Stock Photo

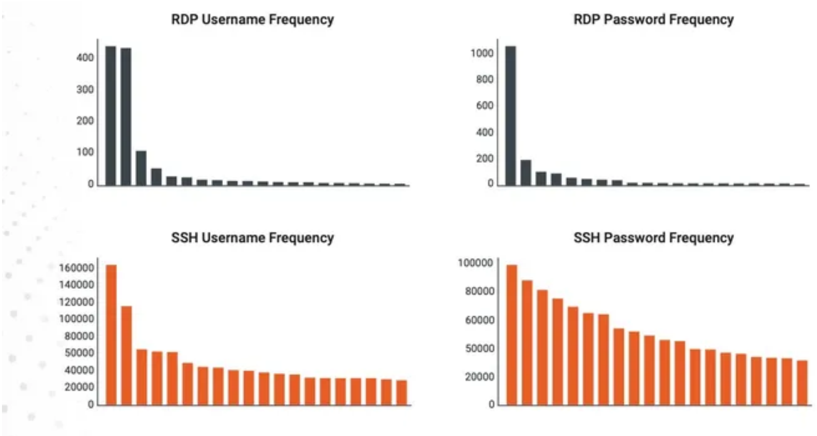
Tens of millions of credential-based attacks targeting two common types of servers boiled down to a small fraction of the passwords that formed a list of leaked credentials, known as the RockYou2021 list.

Vulnerability management firm Rapid7, via its network of honeypots, recorded every attempt to compromise those servers over a 12-month period, finding that the attempted credential attacks resulted in 512,000 permutations. Almost all of those passwords (99.997%) are included in a common password list — the RockYou2021 file, which has 8.4 billion entries — suggesting that attackers, or the subset of threat actors attacking Rapid7's honeypots, are sticking to a common playbook.

The overlap in all the attacks also suggest attackers are taking the easy road, says Tod Beardsley, director of research at Rapid7.

"We know now, in a provable and demonstrable way, that nobody — 0% of attackers — is trying to be creative when it comes to unfocused, untargeted attacks across the Internet," he says. "Therefore, it's very easy to avoid this kind of opportunistic attack, and it takes very little effort to take this threat off the table entirely, with modern password managers and configuration controls."

Every year, security firms present research suggesting users are continuing to pick bad passwords. In October 2021, for example, a cybersecurity researcher in Tel Aviv, Israel, found he could recover the passwords to 70% of the wireless networks as he pedaled past, often because they used a cellphone number as the password. In 2019, an evaluation of passwords leaked to the Internet found that the top password was "123456," followed by "123456789" and "qwerty," although it's unclear whether those leaks included old or rarely used accounts without password policies.



Attackers tend to guess the same common passwords. Source: Rapid7

In this case, however, Rapid7 researchers focused on the common passwords used by attackers rather than defenders, so the analysis applies to attackers' guesses in brute-force attacks. Such attacks have risen dramatically during the COVID-19 pandemic, with password-guessing becoming the most popular method of attack in 2021, according to an analysis by cybersecurity firm ESET.

"With the increasing adoption of both remote work and cloud infrastructures, the number of people accessing corporate information systems across the internet has skyrocketed," Rapid7 stated in its report. "As with so many things in security, the addition of convenience and complexity has made the task of protecting these systems far more challenging."

One Year, a Half-Million Passwords

Rapid7's research used credential data gathered from its Remote Desktop Protocol (RDP) and Secure Shell (SSH) honeypots between Sept. 10, 2021, and Sept. 9, 2022, detecting tens of millions of attempts to connect to the company's honeypots. The vast majority of attacks attempted to gain access to the SSH honeypots, with 97% of the more than 500,000 unique passwords targeting the mock SSH servers, according to Rapid7. The attacks targeting both SSH and RDP came from about 216,000 unique source IP addresses.

The half-million passwords represent less than a 100th of a percent of the permutations in the RockYou21 data set.

"The traffic we're seeing is indicating that these are off-the-shelf attacks with essentially no custom configuration," Beardsley says. "To put it another way, if there was any customization that ventured beyond the stock set of passwords, we would have seen it in these samples."

While the data says little about whether users are selecting poor passwords, the selection does indicate that attackers are taking the simplest path in their attacks. As is clear from the data, attackers are not attempting every entry on the RockYou2021 list, but a much smaller number. In addition, only a handful of passwords and usernames are the most common, dominating the distribution of passwords.

Top RDP usernames are "administrator," "user," and "admin," while the top SSH usernames are "root," "admin," and "nproc." Bad passwords — such as "admin," "password," "123456," and an empty string indicating no password — are the most popular passwords attempted by attackers.

Attackers Just Assume Users Use "Lame" Passwords

The study didn't reflect poor password creation by users but rather that attackers believe that trying a few poorly selected passwords against their targets are a worthwhile guessing game, says Rapid7's Beardsley.

"We can't say precisely how successful attackers are with these lists of lame passwords, but basic economics tells us that they must be getting at least some value out of these attacks, or else we wouldn't be seeing millions of attempts over the year," he says. "My suspicion is that whoever is running these bots are running these attacks essentially at very low cost, and it's worthwhile enough to run this kind of attack with only occasional wins."

Organizations should continuously monitor systems for default and easily guessable passwords, which means running the RockYou2021 list of stolen credentials against exposed and internal systems. Rapid7 also recommends paying particular attention to external-facing SSH and RDP servers, as well as Internet of Things systems that may not have easy-to-change passwords.

In addition, companies should teach employees to use password managers to make strong, unique password creation easy, Beardsley says.

"By utilizing a password manager, you have the ability to generate a completely random password — one that certainly isn't in the RockYou set — and have a different one for every service you offer," he says. "It all depends on being aware of the threat, but once you