CYBER FACTS

BRUTE-FORCE RDP ATTACKS

THREATLOCKER

WHAT IS RDP?

RDP (remote desktop protocol) is used to connect to an employee's desktop over a network connection. It's often used by IT support teams troubleshooting an issue.

WHAT IS A BRUTE FORCE ATTACK?

A brute-force attack occurs when a hacker uses automated tools to cycle through multiple username and password combinations in an attempt to guess the computer's login credentials

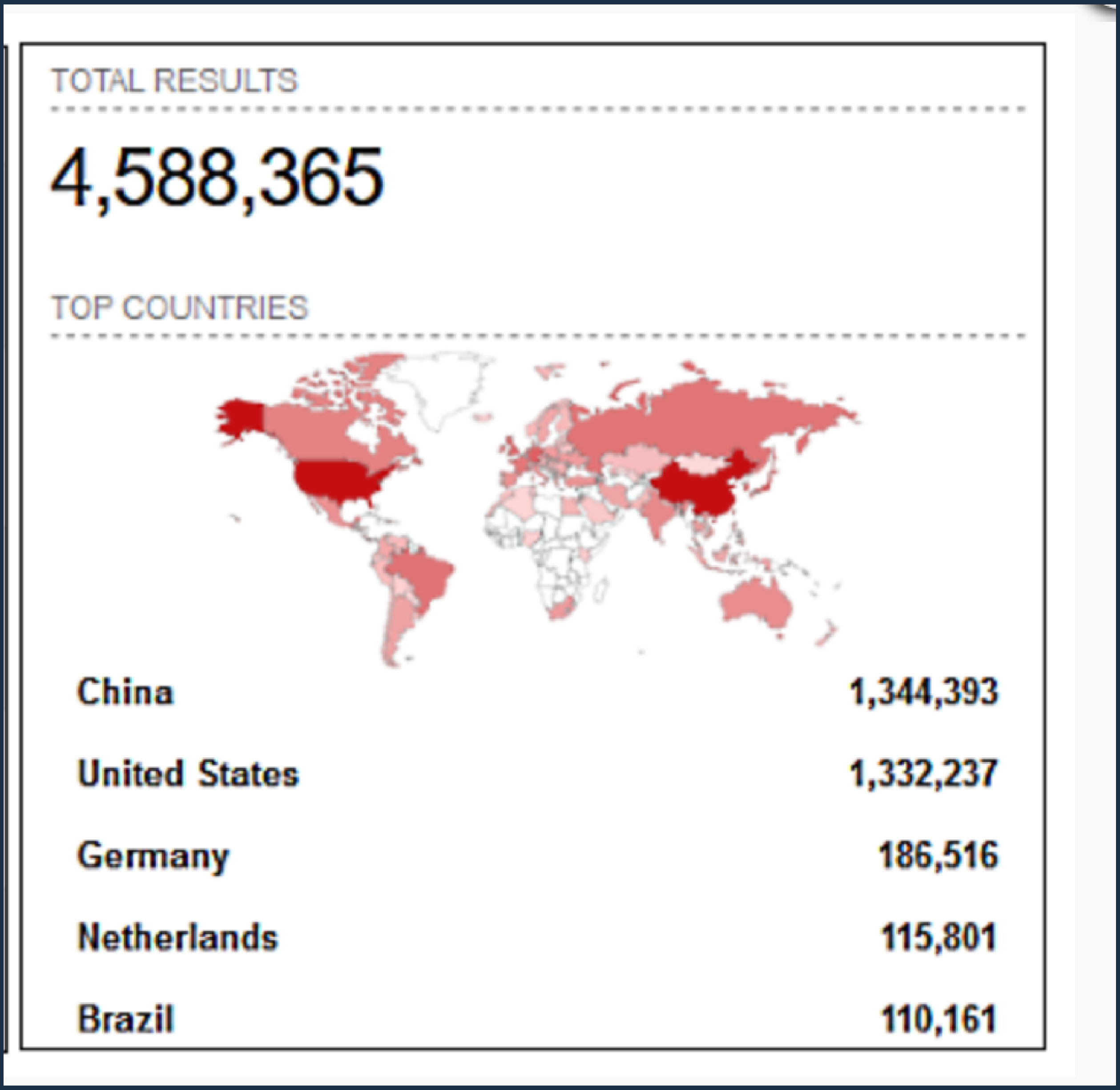
WHY ARE THESE ATTACKS INCREASING?

This is likely a result of attackers looking to take advantage of unprecedented numbers of employees working from home.

HOW FREQUENT ARE THESE ATTACKS?

In the United States alone, brute-force attacks targeting RDP servers have increased from 200,000 per day in early March to over 1.3 million as of mid-April 2020.

OVER 4.5 MILLION DEVICES ARE EXPOSING RDP TO THE INTERNET



TOTAL RESULTS

4,588,365

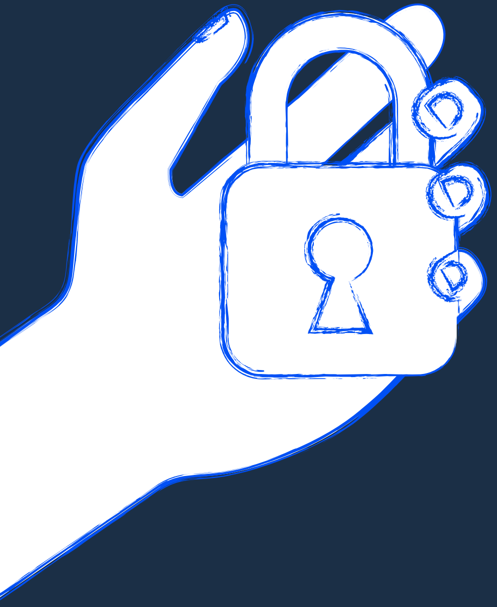
TOP COUNTRIES

China	1,344,393
United States	1,332,237
Germany	186,516
Netherlands	115,801
Brazil	110,161

*BinaryEdge

WHAT HAPPENS DURING AN RDP ATTACK

Once an attacker is in your machine, they use this opportunity to steal your sensitive data, drop malware, and move laterally across your organization's network.



ADDITIONAL FACTS

- In 2017, over 85,000 RDP servers were available for sale on the dark web
- Hacked servers on the dark web marketplace are sold for an average of $6
- An open RDP port is a common attack vector in a ransomware attack

TIPS TO SECURE YOUR RDP SERVERS

- If you don't need RDP, restrict it from running
- Make sure you close port 3389
- Enforce strong and unique passwords
- Use two-factor authentication
- Enable Network Level Authentication (NLA)

FOR MORE SECURITY TIPS VISIT: THREATLOCKER.COM

THREATLOCKER