

Phát hiện và ngăn chặn hơn 47,6 triệu tấn công brute force tại Việt Nam

10:01 05/12/2021

Các chuyên gia cho rằng nửa đầu năm 2021 là giai đoạn các doanh nghiệp Việt Nam đẩy mạnh ứng dụng công nghệ thông tin và chuyển đổi số là một trong những nguyên nhân gia tăng các cuộc tấn công brute force.

Từ tháng 1 đến tháng 6 năm 2021, Kaspersky đã phát hiện và ngăn chặn tổng cộng 47.602.256 tấn công brute force vào giao thức Remote Desktop Protocol (RDP - giao thức kết nối máy tính từ xa) tại Việt Nam.

Theo thống kê về RDP từ Kaspersky, con số này chiếm 42% các nỗ lực tấn công nhằm vào những người dùng sử dụng giải pháp của Kaspersky ở khu vực Đông Nam Á có cài đặt RDP của Microsoft trên máy tính.

Tấn công brute force sử dụng thủ thuật đoán thử đúng - sai để dò tất cả các tổ hợp có thể để tìm ra thông tin đăng nhập, khóa mã hóa dữ liệu hoặc tìm ra một trang web ẩn. Giao thức RDP là một giao thức độc quyền được phát triển bởi Microsoft, cung cấp cho người dùng giao diện để kết nối với một máy tính khác thông qua kết nối mạng.

Dù brute force là phương pháp tấn công không mới nhưng nó vẫn hiệu quả và phổ biến với các hacker. Bằng cách nhắm mục tiêu vào một thiết bị chạy hệ điều hành Windows và sử dụng RDP, sau đó tìm cặp mật khẩu hoặc thông tin đăng nhập RDP chính xác, các hacker có thể truy cập từ xa vào máy chủ và thu lại nhiều lợi ích như: Thu lợi từ quảng cáo, thu thập dữ liệu hoạt động, đánh cắp dữ liệu cá nhân, phát tán phần mềm độc hại gây gián đoạn công việc, tấn công hệ thống để thực hiện các hoạt động độc hại và gây ảnh hưởng xấu đến danh tiếng trang web.



Ảnh minh họa. (Ảnh: intrenet)

So với cùng kỳ năm 2020, số nỗ lực tấn công người dùng thông qua RDP tại Việt Nam tăng 37%. Lý giải nguyên nhân gia tăng các cuộc tấn công brute force, các chuyên gia cho rằng nửa đầu năm 2021 là giai đoạn các doanh nghiệp Việt Nam đẩy mạnh ứng dụng công nghệ thông tin và chuyển đổi số.

Hơn nữa, tình hình phức tạp của dịch bệnh cũng tạo cơ hội cho tội phạm mạng lợi dụng việc các công ty gấp rút chuyển sang hình thức làm việc tại nhà và thiếu sự chuẩn bị cũng như cấu hình máy chủ RDP kém để thực hiện việc tấn công brute force.

Khi tình trạng làm việc tại nhà sẽ có thể tiếp tục, Kaspersky khuyến nghị người sử dụng lao động và doanh nghiệp thực hiện các biện pháp bảo vệ dưới đây: Hãy thiết lập một mật khẩu mạnh; chỉ truy cập RDP thông qua VPN của doanh nghiệp; kích hoạt Network Level Authentication (NLA); nếu có thể, hãy bật xác thực hai yếu tố; nếu không sử dụng RDP, hãy tắt nó và đóng cổng 3389; sử dụng một giải pháp bảo mật đáng tin cậy.

Các công ty cần giám sát chặt chẽ các chương trình đang được sử dụng và cập nhật chúng trên tất cả các thiết bị của công ty một cách kịp thời. Đây không phải là công việc dễ dàng đối với nhiều công ty hiện nay, bởi vì quá trình chuyển đổi vội vàng sang làm việc từ xa đã buộc nhiều người phải cho phép nhân viên làm việc hoặc kết nối với các tài nguyên của công ty từ máy tính tại

nhà của họ.

Các chuyên gia cũng khuyến nghị đào tạo cơ bản về giữ an toàn cho máy tính và hệ thống mạng cho nhân viên của công ty, giúp nhân viên nhận biết các kiểu tấn công phổ biến nhất xảy ra trong công ty và cung cấp kiến thức cơ bản trong việc nhận biết các email, trang web và các tin nhắn đáng ngờ; Sử dụng các mật khẩu mạnh, phức tạp và các mật khẩu khác nhau để truy cập vào các tài nguyên của công ty; Sử dụng xác thực đa yếu tố hoặc xác thực hai yếu tố, đặc biệt khi truy cập vào thông tin tài chính hoặc đăng nhập vào mạng công ty.

Đồng thời, nếu có thể, hãy sử dụng mã hóa trên các thiết bị được sử dụng cho mục đích công việc; cho phép truy cập RDP thông qua VPN công ty; luôn chuẩn bị các bản sao lưu của dữ liệu quan trọng; sử dụng giải pháp bảo mật doanh nghiệp đáng tin cậy với khả năng bảo vệ khỏi mối đe dọa mạng như Kaspersky Endpoint Security for Business.

Hà Trần