TẤN CÔNG TỪ CHỐI DỊCH VỤ VẪN LÀ NGUY CƠ SỐ MỘT

Dù hiện nay tình trạng phát tán virus đã trở nên phổ biến, 90% doanh nghiệp khẳng định những cuộc tấn công DDoS đang là vấn đề phiền toái và thường gặp nhất trong công ty.

Tấn công từ chối dịch vụ (DDoS/ DoS - denial of service attack) là kiểu tấn công khiến một hệ thống máy tính hoặc một mạng bị quá tải, dẫn tới không thể cung cấp dịch vụ hoặc phải dừng hoạt động. Sơ khai nhất là hình thức DoS (Denial of Service), lợi dụng sự yếu kém của giao thức TCP, tiếp đến là DDoS - tấn công từ chối dịch vụ phân tán, và gần đây là DRDoS - tấn công theo phương pháp phản xạ phân tán (Distributed Reflection Denial of Service). Nhiễm độc DNS (DNS cache poisoning) là thủ thuật lừa một máy chủ DNS tin rằng nó vừa nhận được một thông tin đáng tin cậy. Một khi server DNS bị nhiễm, thông tin sẽ lưu lại (cache) và sau đó mở rộng ảnh hưởng sang những người sử dụng server đó.

Hãng Arbor Networks (Mỹ) đã thực hiện một cuộc điều tra bảo mật ISP toàn cầu với sự tham gia của 36 nhà cung cấp dịch vụ Internet ở Mỹ, châu Âu và châu Á. Kết quả cho thấy hình thức tấn công thịnh hành nhất là các trận DDoS qua những gói thông tin UDP và TCP SYN từ mạng máy tính bị khống chế (zombie). Hai mối đe dọa tiếp theo là sâu chứa mã nguy hiểm và nhiễm độc DNS (DNS poisoning). Tuy nhiên, nếu xét về khả năng gây mức độ rủi ro cao cho công ty thì sâu mạng vẫn là nguy cơ hàng đầu. Dù đã xuất hiện và tung hoành trong vài năm trở lại đây, chỉ có 29% các hãng ISP trang bị phương pháp ngăn chặn và dò tìm tấn công từ chối dịch vụ tự động. Phần đông chỉ nhận biết được rắc rối khi một khách hàng nào đó liên hệ với họ yêu cầu trợ giúp. Phương tiện chính để đối phó với DDoS hiện nay vẫn là sử dụng danh sách kiểm soát ALCs (Access Control Lists), nhưng mặt khác nó cũng sẽ chặn khả năng truy cập mạng. Động lực của việc thực hiện tấn công từ chối dịch vụ là tống tiền, âm mưu chống lại các công ty, thậm chí để gián điệp... T.N. (theo TechWorld)