NGƯỜI DÙNG MỚI LÀ MỤC TIÊU TRỌNG TÂM CỦA TIN TẶC

Tin tặc đang chuyển mục tiêu tấn công sang người sử dụng thay vì tấn công vào các hệ thống. Minh chứng rõ ràng nhất cho xu hướng chuyển đổi mục tiêu tấn công trong giới tin tặc chính là việc liên tiếp công bố các lỗi bảo mật trong bộ ứng dụng Microsoft

Tin tặc đang chuyển mục tiêu tấn công sang người sử dụng thay vì tấn công vào các hệ thống. Minh chứng rõ ràng nhất cho xu hướng chuyển đổi mục tiêu tấn công trong giới tin tặc chính là việc liên tiếp công bố các lỗi bảo mật trong bộ ứng dụng Microsoft Office và hàng loạt các mối đe doạ bảo mật đến từ các loại văn bản độc hại có khả năng khai thác các lỗi bảo mật đó. Thực tế đó cũng nói lên một điều là bọn tin tặc dường như cũng đã tự động hoá được việc phát hiện và khai thác các lỗi bảo mật. Mục tiêu là người dùng Alfred Huger - một chuyên gia cao cấp của hãng bảo mật Symantec - khẳng định: "Tin tặc đang nhắm mục tiêu tấn công vào người dùng hơn là vào các hệ thống. Cái mà chúng tìm kiếm không phải là máy chủ mà chúng tìm kiếm tên đăng nhập và địa chỉ email". "Khó có thể nhận biết được một con người cụ thể từ một trang web. Chính vì thế mà những kẻ tấn công đã nhắm mục tiêu đến một công ty cụ thể, chúng tập trung vào cuộc tấn công hơn, chúng đang chuyển sang tấn công các ứng dụng máy khách cụ thể như Microsoft chẳng hạn." Huger giả lập một mô hình tấn công có mục tiêu thông qua việc khai thác lỗi bảo mật trong Office như sau: "Một kẻ tấn công có thể tìm thấy tên và địa chỉ email của một nhân viên tài chính cấp thấp của một công ty, từ một thông cáo báo chí chẳng hạn. Sau đó chúng sẽ giả mạo là người quản lý tài chính của công ty đó để gửi cho nhân viên nói trên một tệp tin Excel. Như vậy, việc người nhân viên cấp thấp đó mở tệp tin Excel của tin tặc ra là rất cao vì anh ta sẽ nghĩ nó được gửi đi từ người quản lý của anh ta. Rõ ràng mức độ thành công của những vụ tấn công như thế này sẽ rất cao". Fuzzer lộ diện Việc liên tiếp phát hiện ra các lỗi bảo mật trong Office đã làm bùng lên sự lo lắng về các công cụ có tên "fuzzer" - một công cụ tự động phát hiện các lỗi bảo mật được phát triển bởi các nhà nghiên cứu bảo mật và tin tặc trong khoảng hơn hai năm qua. Tuy nhiên, công cụ này mới chỉ vừa được công chúng biết đến. "Một công cụ fuzzer sẽ gửi đi bất kỳ một loại giá trị dữ liệu tới đầu vào của bất kỳ một chương trình nào để phát hiện xem có trục trặc gì xảy ra không. Đây là công cụ được dùng phổ biến trong việc phát hiện các lỗi bảo mật tràn bộ nhớ đệm. Và nó cũng là một giải pháp nhanh chóng và hiệu quả nhất trong việc phát hiện các lỗi bảo mật," Huger cho biết. Huger cho rằng nhờ có HD Moore mà mọi người chúng ta mới được biết đến fuzzer. Moore - một trong những nhà phát triển đi đầu trong dự án mã nguồn mở Metasploit Framework - vừa mới khởi động dự án "mỗi ngày một lỗi bảo mật" và khẳng định ông đã dùng khá nhiều fuzzer để phát hiện các lỗi bảo mật đó. Microsoft cũng là một trong số những hãng dành nhiều thời gian và tiền bạc nhất cho fuzzer, Huger khẳng định. Chuyên gia này tin rằng chính Windows Vista cũng được thử nghiệm bằng công cụ fuzzer. "Tôi cho rằng điều này sẽ mang lại một nền tảng tốt hơn cho Vista," Huger khẳng định. "Nhưng như thế không phải là đã chấm dứt lo ngại về lỗi bảo mật. Tin tặc vẫn phát hiện được các lỗi trong Vista vì đã có những đoạn mã mới." Hoàng Dũng