# CÔNG NGHIỆP BẢO MẬT SẼ THAY ĐỔI?

Liệu có điều gì đáng phải sợ hãi trong thế giới bảo mật công nghệ thông tin (CNTT)? Từ nhiều năm rồi McAfee, Symantec cũng như các nhà sản xuất phần mềm phòng chống virus đã không ngừng trợ giúp các công ty trong việc giữ cho hệ thống mạng của mình

Liệu có điều gì đáng phải sợ hãi trong thế giới bảo mật công nghệ thông tin (CNTT)? Từ nhiều năm rồi McAfee, Symantec cũng như các nhà sản xuất phần mềm phòng chống virus đã không ngừng trợ giúp các công ty trong việc giữ cho hệ thống mạng của mình khỏi sự tấn công của virus, trojan và các loại đoạn mã chương trình độc hại có thể gây ra những thiệt hại đáng kể. Nhưng đến giờ vẫn những "hiệp sĩ bảo vệ máy tính" đó nhưng họ lại đang kinh doanh những phần mềm bảo mật không còn đủ khả năng chống lại các cuộc tấn công nữa, bản thân những phần mềm đó cũng bị lợi dụng để tấn công người sử dụng. Những lỗ hổng bảo mật mới được phát hiện gần đây trong các phần mềm bảo mật của McAfee, Symantec, và Trend Micro cho phép tin tặc có thể chiếm quyền điều khiển máy tính. Trong khi hầu hết các phần mềm chống virus đều được phân phối thông qua việc tải qua mạng khiến cho tin tặc khó có thể kiếm được mã các chương trình này. Không những thế những lỗi bảo mật này cũng đã làm nổi lên những vấn đề với định hướng phản ứng bảo mật của ngành công nghiệp chống virus. Đây chính là cơ hội mới cho Microsoft bước chân vào thị trường bảo mật. Hồi đầu tuần, Symantec chính thức tiết lộ ra thư viện chống virus của hãng này hoàn toàn có thể bị tấn công thông qua lỗi bảo mật tràn bộ nhớ đệm. Tin tặc hoàn toàn có thể lợi dụng khai thác lỗ hổng bảo mật này để chiếm quyền điều khiển máy tính của người dùng sử dụng thư viện kiểu này. Lỗi bảo mật này ảnh hưởng đến một loại các sản phẩm của Symantec như Symantec Norton SystemWorks, Symantec Norton Internet Security, Symantec Norton AntiVirus, Symantec Gateway Security, Brightmail Anti-Spam, và Symantec Client Security. Chuyên gia nghiên cứu bảo mật Alex Wheeler là người đầu tiên thông báo lỗi bảo mật trong các sản phẩm bảo mật cho Symantec. Trên thực tế, từ hồi tháng 2 khi còn là một thành viên của nhóm nghiên cứu X-Force thuộc Internet Security Systems đối thủ cạnh tranh của Symantec, Wheeler đã phát hiện ra lỗi bảo mật trong thư viện chống virus ảnh hưởng đến Brightmail AntiSpam, AntiVirus Corporate Edition cũng như các sản phẩm khác của Symantec. Lỗi bảo mật này có thể cho phép tin tặc khai thác module DEC2EXE, một bộ phận động cơ quét có thể truy cập vào Ultimate Packer để thực hiện các eXecutables trong các tệp tin nén và gây ra tình trạng tràn bộ nhớ đệm. Trong khi Symantec đã nỗ lực để vá lỗ hổng bảo mật trong các sản phẩm của mình thì đối thủ cạnh tranh McAfee trong tuần này cũng chính thức cảnh báo người sử dụng rằng một loạt các phiên bản phần mềm quét virus của hãng này mắc lỗi bảo mật cho phép "ghi đè tệp tin mã nhị phân" (arbitrary file overwrite) cho phép tin tặc có thể tạo và sửa đổi các tệp tin nhị phân để ghi các thông tin dữ liệu lên máy tính của người sử dụng. McAfee đã nhanh chóng cho ban hành bản vá lỗi bảo mật này. Không chỉ có thể ngày cả phần mềm bảo mật PC-Cillin Internet Security Antivirus của Trend Micro cũng không là ngoại lệ. VeriSign iDefense đã phát hiện ra sản phẩm bảo mật của Trend Micro mắc một lỗi bảo mật cho phép tin tặc có thể tăng quyền truy cập người sử dụng hoặc là vô hiệu hoá khả năng bảo mật. Lỗi bảo mật này ảnh hưởng đến các phiên bản 12.00 và 12.44. Tin tặc có thể lợi dụng lỗi bảo mật này để ghi đè các mã nhị phân hoạt động ở cấp hệ thống cho phép chúng chiếm đoạt quyền điều khiển hệ thống máy tính của người dùng. Như vậy, những vấn đề mà McAfee, Symantec, Trend Micro cũng như sản phẩm của các hãng bảo mật khác cho thấy những sản phẩm này không hề tốt hơn các phần mềm khác ở cấp độ viết mã phần mềm, Burton Group chuyên gia phân tích của Fred Cohen cho biết. Nhưng kể từ khi tin tặc không thể dễ dàng

nhúng các đoạn mã vào trong các phần mềm được phát tán qua mạng thì những sự tấn công khai thác mã bảo mật có thể bị khai thác Vấn đề này đặt ra một câu hỏi về việc chúng ta đặt bao nhiêu niềm tin vào các nhà cung cấp phần mềm bảo mật này cũng như vào mô hình cập nhật mà họ đang thực hiện. Đó phải là một biện pháp phản ứng để bảo đảm nhưng nó cũng phải là một biện pháp phải dựa trên sự tin tưởng của người sử dụng vào các nhà cung cấp phần mềm khi họ phải cài đặt phần mềm lên máy tính. Cohen đặt ra một câu hỏi: "Điều gì sẽ xảy ra khi có một người nào đó ở ngay trong chính các hãng bảo mật này cài đặt một con trojan lên hệ thống của họ?" Trong khi đó với những lỗi bảo mật này sẽ khiến cho các chuyên gia chống virus chứng minh được rằng phần mềm bảo mật của họ là tốt nhất. Microsoft lại đang ngấp nghé bước chân vào thị trường này. Gartner VP cùng với người đồng nghiệp John Pescatore cho biết: "Nhiều hãng kinh doanh phần mềm chống virus nói rằng 'Vâng, đúng, ai mua phần mềm chống virus của Microsoft khi mà bản thân họ không thể giữ bảo mật cho chính sản phẩm của họ'". Nhưng nếu sản phẩm của Microsoft rẻ hơn của các nhà phát triển khác thì sao trong khi chính những nhà phát triển đó lại không chứng minh được rằng sản phẩm của họ có chất lượng cao hơn của Microsoft. Thất bại là điều hoàn toàn dễ nhận thấy. Một số sự kiện gần đây có thể thổi bùng lên ngọn lửa làm thay đổi trong mức độ tin tưởng vào mô hình cài đặt và cập nhật của các phần mềm chống virus. Giải pháp về lâu về dài để chống lại thảm hoạ cho các phần mềm chống virus phải là mô hình sáng kiến tin tưởng mà ở đó các khoá kĩ thuật số, chứng chỉ và mật khẩu được lưu trữ trên các vi xử lý trong máy tính, máy chủ và phần cứng. "Đây sẽ là những ảnh hưởng quan trọng đối với thị trường chống virus, phần mềm gián điệp nguy hiểm trong thời gian từ 5 đến 7 năm tới," Cohen cho biết. Tại sao lại phải có một thời gian lâu đến như vậy? Bởi vì 15 triệu máy tính mà các hãng kinh doanh PC cung cấp không đủ gây ảnh hưởng. "Bạn cần phải có ít nhất 100 triệu máy tính tin tưởng," Cohen cho biết. Điều này sẽ không thể xảy ra cho đến tận khi nào mà vòng tiếp theo của sự thay thế PC xảy ra - một vòng quay cần thời gian từ 3 đến 5 năm