BOTWARE HOÀNH HÀNH TRONG THÁNG 8

Hãng bảo mật Panda Software cảnh báo người dùng không chỉ nên thận trọng trước hiểm hoạ bảo mật đến từ virus mà còn cả các loại phần mềm độc hại khác. Panda cho biết tháng 8 là tháng thống trị của các loại phần mềm bot (botware) - loại phần mềm chuyên di

Hãng bảo mật Panda Software cảnh báo người dùng không chỉ nên thận trọng trước hiểm hoạ bảo mật đến từ virus mà còn cả các loại phần mềm độc hại khác. Panda cho biết tháng 8 là tháng thống trị của các loại phần mềm bot (botware) - loại phần mềm chuyên di “gieo mầm” xây dựng các hệ thống botnet và zombie phục vụ mục đích đen tối của bọn tội phạm mạng. Có thể nói bọn tội phạm ngày một thận trọng hơn. Chúng không còn muốn tổ chức những vụ tấn công lớn hay những “đại dịch virus” nữa vì những hành động như thế này sẽ thú hút được sự chú ý của báo chí và chúng dễ dàng rơi vào tay của các hãng bảo mật. Nhờ đó mà người dùng sẽ càng cảnh giá hơn với chúng. Tác giả các loại phần mềm độc hại giờ đây nhắm đến mục tiêu tấn công các hệ thống của người dùng mà không gây ra bất kỳ một sự nghi ngờ chú ý nào với các phần mềm độc hại có thể mang lại lợi nhuận thực cho chúng. Minh chứng rõ ràng nhất chính là lỗi bảo mật Microsoft MS06-040. Lỗi bảo mật này hoàn toàn có thể gây là một đại dịch virus nếu nó được phát hiện vài năm trước đây. Nhưng giờ đây thì không. Hàng ngày đều có các loại phần mềm độc hại được phát hiện là nhắm mục tiêu khai thác lỗi bảo mật đó. Nhưng chúng lại khai thác một cách bí mật khiến không một ai nhận biết. Không những thế MS06-040 còn tạo ra sự hoành hành của botware. Chính lỗi bảo mật này là nguyên nhân khiến cho số lượng các Zombie PC tăng mạnh trong thời gian qua. Phần mềm độc hại phổ biến nhất trong tháng 8 là Sdbot.ftp - một biến thể của dòng sâu máy tính Sdbot có khả năng lây nhiễm thông qua kết nối FTP. Đứng ở vị trí thứ 2 và thứ 3 lần lượt là Jupillites.G và Netsky.P tấn công một lỗi bảo mật trong trình duyệt Internet Explorer. Các vị trí tiếp theo thuộc về Sinowal.BV Trojan và Bagle.pwdzip. Đứng vị thứ 6 là W32/Parite.B - loại lâu sâu biến hình lây nhiễm lên các tệp tin EXE và thứ 7 là con trojan Downloader.IOL Trojan với chức năng tải các tệp tin độc hại khác lên hệ thống bị nhiễm. Cuối cùng là Exploit/Metafile Ailis.A.worm. Hoàng Dũng