SÂU MỚI "ĐỘI LỐT" PHẦN MỀM WGA CỦA MICROSOFT

Các chuyên gia bảo mật vừa phát hiện một malware mới giả mạo phần mềm chuyên "đánh hơi" các phiên bản Windows lậu của Microsoft.

Nguồn: 24x7updates

Theo phân loại của chuyên gia Graham Cluley,
Các chuyên gia bảo mật vừa phát hiện một malware mới giả mạo phần mềm chuyên "đánh hơi" các phiên bản Windows lậu của Microsoft.

Nguồn: 24x7updates

Theo phân loại của chuyên gia Graham Cluley, hãng Sophos thì malware này là một dạng sâu phát tán thông qua chương trình chat IM của AOL. Sophos đã đặt tên cho nó là W32.Cuebot-K, một biến thể mới của họ malware Cuebot. W32.Cuebot-K là một con sâu rất "đa năng". Sau khi cài đặt, nó sẽ ngay lập tức tìm cách kết nối với 2 website mặc định - một dấu hiệu cho thấy mục tiêu cuối cùng của nó là tìm cách download tiếp các malware khác về máy. Chưa hết, Cuebot-K còn có thể vô hiệu hóa các phần mềm diệt virus, tắt tường lửa Windows, thực hiện các cuộc tấn công từ chối dịch vụ cơ bản, dò quét file trong máy tính .... Thường thì những con sâu phát tán qua chương trình chat thường xuất hiện dưới hình thức một thông điệp hoặc đường link gửi đi từ bạn bè, dụ người dùng click vào và kích hoạt. Về phần mình, Cuebot-K phát tán bằng cách tự gửi nó đi dưới dạng một file có tên "wgavn.exe" nhưng không có thông điệp kèm theo. Khi cài đặt xong xuôi, Cuebot-K sẽ đăng ký như một dịch vụ driver thiết bị hệ thống mới là wgavn, tức Windows Genuine Advantage Validation Notification. Điều mỉa mai là Cuebot-K lại xuất hiện vào đúng thời điểm mà WGA - phần mềm nó giả dạng - đang bị chỉ trích dữ dội vì hoạt động không khác gì một spyware. Phần mềm này chuyên thu thập các dữ liệu về phần mềm và phần cứng trong máy tính người dùng rồi đối chiếu nó với một cơ sở dữ liệu về các hệ điều hành có phép. Nếu phát hiện ra bản Windows lậu, nó sẽ "truyền tin" về tổng hành dinh. Microsoft khi đó sẽ cảnh cáo người dùng và cắt bỏ một số dịch vụ download miễn phí dành cho họ. Thiên Ý