

CẢNH BÁO NGUY CƠ MẤT AN TOÀN THÔNG TIN TRÊN MỘT SỐ DÒNG MÁY TÍNH LENOVO

Trung tâm Ứng cứu khẩn cấp máy tính Hoa kỳ (USCERT) đã công bố phát hiện một số dòng máy tính của Lenovo sản xuất từ tháng 9/2014 đã bị cài đặt trước phần mềm độc hại dạng adware có tên là Superfish VisualDiscovery (gọi tắt là Superfish). Phần mềm này có thể thu thập thông tin từ các truy cập trên các máy tính bị cài đặt Superfish ngay cả khi các luồng dữ liệu đã được mã hoá bằng giao thức HTTPS và chèn thông tin quảng cáo vào lưu lượng web của người dùng. Do phần mềm Superfish sử dụng chứng thư số tin cậy từ hệ thống, trình duyệt sẽ không hiển thị bất kỳ cảnh báo nào về việc lưu lượng web đã bị giả mạo. Mặc dù Công ty Lenovo tuyên bố đã gỡ bỏ phần mềm trên ra khỏi các máy tính của hãng sản xuất sau tháng 01/2015, song những máy tính đã xuất xưởng trước đây vẫn có thể đã bị cài đặt phần mềm Superfish.

Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam (VNCERT) đánh giá đây là một nguy cơ mất an toàn thông tin nghiêm trọng, cho phép tin tặc giả mạo SSL, tấn công đánh cắp thông tin trong các ứng dụng thư điện tử, giao dịch qua mạng v.v..

Trung tâm VNCERT kính đề nghị Quý đơn vị phổ biến, cảnh báo và chỉ đạo thực hiện rà soát, gỡ bỏ, vô hiệu hoá phần mềm trên để bảo đảm an toàn thông tin. Trung tâm VNCERT cung cấp cảnh báo và hướng dẫn tại địa chỉ <http://vncert.gov.vn/>.

Mọi thông tin chi tiết xin vui lòng liên hệ:

- Phòng Kỹ thuật hệ thống – Trung tâm VNCERT
- Điện thoại : 0436404424

HƯỚNG DẪN KHẮC PHỤC NGUY CƠ MẤT AN TOÀN THÔNG TIN TRÊN MỘT SỐ DÒNG MÁY TÍNH LENOVO

1. Kiểm tra một số dòng máy tính Lenovo bị cài đặt Superfish. Tham khảo tại địa chỉ:

<https://support.lenovo.com/us/en/mcafeesubscription>

2. Gỡ bỏ phần mềm Superfish và các chứng thư số liên quan:

- Sử dụng phần mềm chống Virus đã được cập nhật

- Tham khảo công cụ do Lenovo cung cấp tại địa chỉ:

https://support.lenovo.com/us/en/product_security/superfish_uninstall

- Tham khảo hướng dẫn của Microsoft tại địa chỉ:

<http://windows.microsoft.com/en-us/windows-vista/view-or-manage-your-certificates>

<https://technet.microsoft.com/en-us/library/cc772354.aspx>

- Tham khảo hướng dẫn của Mozilla tại địa chỉ:

https://wiki.mozilla.org/CA:UserCertDB#Deleting_a_Root_Certificate