Hàng loạt máy tính tại Việt Nam bị nhi□m virus đào ti□n □o, nguyên nhân và cách kh□c phục!

Các loại virus đào ti□n □o đang phát tán r□t nhanh trên internet hiện nay. Theo th□ng kê c□a Bkav hiện □ Việt Nam có kho□ng 750.000 máy tính bị nhi□m virus W32.AdCoinMiner. Máy tính bị nhi□m sẽ bị ki□m soát b□i Hacker và s□ dụng với mục đích đào ti□n □o.

Theo th□ng kê thì việc các máy tính bị lây nhi□m virus đào ti□n □o nhi□u nh□t nguyên nhân do hacker đã chèn mã độc qua trang rút gọn link ki□m ti□n có chứa qu□ng cáo **adf.ly**

Adf.ly là gì ?

Adf.ly là một website **rút gọn link ki□m ti□n** đã có từ r□t lâu có th□ nói đây là một trang rút gọn link lâu đời và có quy mô lớn nh□t th□ giới. Tuy nhiên hạn ch□ c□a Adf.ly là cho phép s□ dụng ifames c□a Website khác đ□ chạy Qu□ng cáo. Lợi dụng đi□u này, các Hacker đã chèn mã đọc vào các trang iframe Qu□ng cáo nhằm mục đích phát tán virus đào ti□n □o. Trước khi đ□n được link đích, máy tính người dùng có th□ đã tự download virus xu□ng trong quá trình t□i Qu□ng cáo mà không h□ hay bi□t. Sau khi bị lây nhi□m, máy tính sẽ bị các hacker chi□m quy□n đi□u khi□n và s□ dụng tài nguyên như CPU, GPU đ□ đào ti□n □o một

cách âm thầm mà người dùng không hề hay biết.

Hàng loạt máy tính tại Việt Nam bị nhiễm virus đào tiền ảo

Sự nguy hiểm của Virus W32.AdCoinMiner (Virus đào tiền ảo)

Một điều cực kỳ nguy hiểm hơn với **virus W32.AdCoinMiner** đó là: sau khi lây nhiễm virus có thể tự động tải thêm mã độc từ Server của Hacker, sau đó ẩn mình với lớp bộc là file hệ thống Windows để tiến hành các hành vi **gián điệp, đánh cắp thông tin, thậm chí xóa dấu vết, xóa dữ liệu….**

Ngoài việc lợi dụng lỗ hổng quảng cáo của **Adf.ly**, các Hacker còn tận dụng lỗ hổng **SMB**(lỗ hổng từ **Win 7** trở đi) để phát tán Virus trên quy mô toàn cầu. **Lỗ hổng SMB** được bị hack tận dụng để phát tán **Virus WannaCry** hồi năm **2017**, đến bây giờ vẫn chưa có cách để giải mã các file bị virus mã hóa. Theo thống kê của **BKAV**, hiện hơn 1 nửa số máy tính tại Việt Nam chưa vá bản sửa lỗi cho Windows để khắc phục lỗ hổng này.

virus đào tiền ảo

Cách phát hiện virus đào tiền ảo trong máy tính của bạn

Bạn cần thường xuyên kiểm tra **CPU, RAM, GPU** xem có bị 100% không. Nếu không sử dụng tác vụ nặng mà **Task Manager** báo **100%** thì chắc chắn là bạn đã bị dính **Virus đào tiền ảo** rồi.

Cách tốt nhất là cài lại Win hoặc sử dụng phần mềm diệt virus cập nhật bản vá mới nhất để quét toàn bộ máy tính.

virus đào ti□n □o- 1

Cách phòng tránh virus đào ti□n □o

Phòng bệnh hơn ch□a bệnh, đ□ tránh máy tính bị dính virus đào ti□n □o. Bạn nên trang bị cho mình ki□n thức nh□t định v□ tin học, đ□ có th□ nhận bi□t được các file nào nên m□, file nào nên xóa ngay lập tức.

Đ□i với các trang rút gọn link **adf.ly** n□u th□y trình duyệt tự động t□i file mặc dù chưa b□ qua bước **skip ads** thì tuyệt đ□i không t□i v□. Ph□i ki□m tra xem tên file c□n t□i v□ có gi□ng với ch□ đích mình mu□n t□i không.

Luôn đ□ ch□ độ Auto Update cho Windows, và cài đặt ph□n m□m diệt virus uy tín Kaspersky, BKAV, Avast…(có b□n quy□n)!