

Một học sinh lớp 12 ở Thanh Hóa dùng mã độc đánh cắp dữ liệu máy tính người dùng toàn cầu

By NLD.COM.VN

Published: 2026-03-24 · Archived: 2026-05-22 02:02:06 UTC

Ngày 24-3, tin từ Công an tỉnh Thanh Hóa cho biết Cơ quan An ninh điều tra Công an tỉnh này vừa khởi tố vụ án, khởi tố 12 bị can (trong đó có 1 học sinh lớp 12) về các tội danh liên quan đến sản xuất, phát tán phần mềm trái phép và xâm nhập hệ thống máy tính.



Công an tỉnh Thanh Hóa tiến hành khám xét nhà N.V.X. - là người lập trình mã độc, cầm đầu đường dây xâm nhập, đánh cắp dữ liệu người dùng máy tính toàn cầu. Ảnh: Công an Thanh Hóa

Theo Công an tỉnh Thanh Hóa, đầu năm 2026, lực lượng an ninh mạng Bộ Công an phối hợp với Công an tỉnh Thanh Hóa phát hiện dấu hiệu của một đường dây chuyên phát tán mã độc nhằm đánh cắp dữ liệu người dùng Internet trên phạm vi toàn cầu. Qua quá trình xác minh, các đối tượng đã tổ chức hoạt động theo quy trình khép kín, từ lập trình, phát tán đến khai thác dữ liệu.

Đáng chú ý, người trực tiếp viết mã độc là N.V.X. (tên nhân vật đã thay đổi, ngụ phường Hạc Thành, tỉnh Thanh Hóa; hiện đang là học sinh lớp 12). Ban đầu, X. tự học lập trình với các ngôn ngữ như Python, C++ để phục vụ nghiên cứu cá nhân. Tuy nhiên, trong quá trình tìm hiểu sâu về hệ điều hành và dữ liệu, đối tượng đã phát triển các đoạn mã có khả năng truy cập, thu thập thông tin nhạy cảm trên máy tính người dùng như cookies, mật khẩu, dữ liệu tự động điền.

Đến năm 2024, X. hoàn thiện bộ mã độc có thể vượt qua các lớp bảo vệ cơ bản và gửi dữ liệu đánh cắp về máy chủ điều khiển. Thông qua mạng xã hội Telegram, X. quen biết Lê Thành Công (Hà Tĩnh), từ đó bắt đầu hợp tác phát triển và phát tán mã độc nhằm trục lợi từ việc đánh cắp tài khoản, đặc biệt là tài khoản Facebook có giá trị thương mại.

Sau đó, X. tiếp tục hợp tác với Phan Xuân Anh (Nghệ An) để phát triển một dòng mã độc mới có tên "PXA Stealers". Theo thỏa thuận, X. chịu trách nhiệm lập trình và cập nhật mã độc, hưởng 15% lợi nhuận, còn các đối tượng khác đảm nhiệm việc phát tán và khai thác dữ liệu. Nhóm này còn tích hợp phần mềm điều khiển từ xa (Pure RAT) vào mã độc, cho phép chiếm quyền điều khiển máy tính nạn nhân.

Theo Công an Thanh Hóa, không dừng lại ở đó, X. còn nhận "đặt hàng" từ một đối tượng khác là Nguyễn Thành Trường để phát triển mã độc mới mang tên "Adonis", với giá 500 USD cùng khoản chia lợi nhuận sau đó. Các mã độc này liên tục được cập nhật để vượt qua hệ thống bảo mật và mở rộng phạm vi lây nhiễm.



Tang vật liên quan tới vụ án. Ảnh: Công an Thanh Hóa

Thủ đoạn phát tán chủ yếu của các đối tượng là gửi email hàng loạt kèm tệp đính kèm chứa mã độc. Các tệp này được ngụy trang dưới dạng file PDF hoặc văn bản thông thường nhưng thực chất là file thực thi (.exe). Khi người dùng mở file, mã độc tự động cài đặt và hoạt động ngầm, thu thập dữ liệu rồi gửi về hệ thống Telegram hoặc máy chủ do nhóm quản lý. Ngoài ra, chúng còn sử dụng danh sách email mua từ các diễn đàn dữ liệu để mở rộng phạm vi tấn công.

Kết quả điều tra cho thấy hơn 94.000 máy tính tại nhiều quốc gia, chủ yếu ở châu Âu, châu Mỹ và một số nước châu Á, đã bị nhiễm mã độc. Dữ liệu thu thập được sử dụng để chiếm quyền tài khoản mạng xã hội, chạy quảng cáo kiếm tiền hoặc bán lại cho bên thứ ba. Tổng số tiền thu lợi bất chính ước tính lên tới hàng chục tỉ đồng.

Hiện vụ án đang được Công an tỉnh Thanh Hóa tiếp tục điều tra, làm rõ.

Source: <https://nld.com.vn/mot-hoc-sinh-lop-12-o-thanh-hoa-dung-ma-doc-danh-cap-du-lieu-may-tinh-nguoi-dung-toan-cau-196260324215720573.htm>