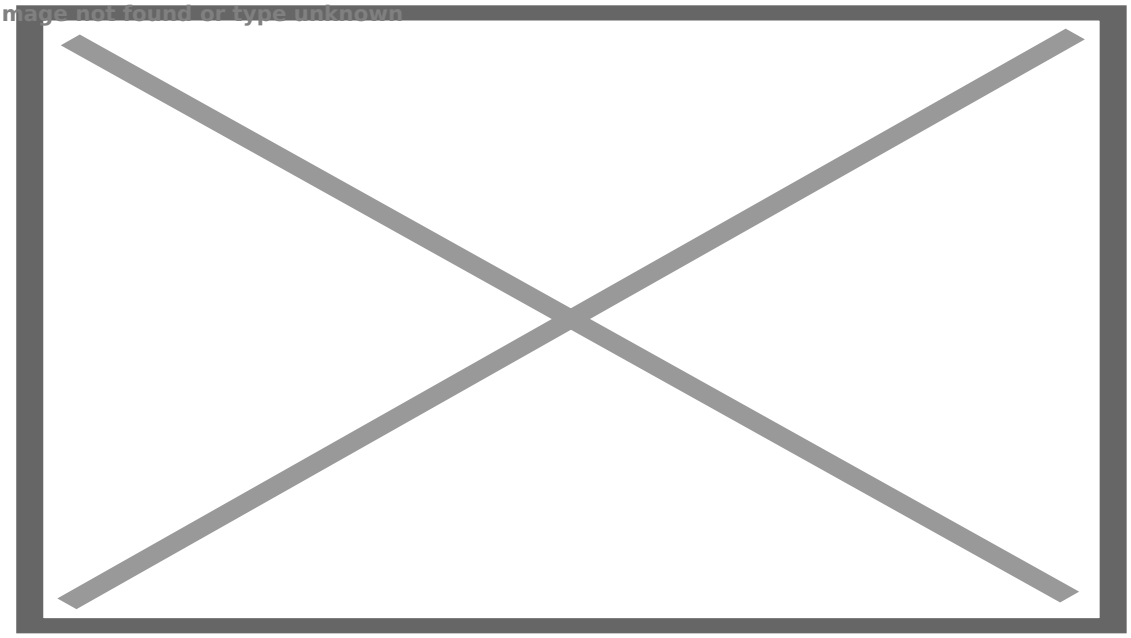
Hacker bán công cụ phát tán phần mềm độc hại thông qua các tập tin torrent

12:28 26/09/2016

Tác giả: Phạm Thùy Dung

Nếu bạn là người thích chia sẻ dữ liệu thông qua torrent thì ngay bây giờ hãy thận trọng với những file torrent đó

Image not found or type unknown



Đây là một công cụ mới được rao bán trên thị trường chợ đen, đang giúp các hacker phát tán phần mềm độc hại thông qua các torrent đó để trao đổi lấy tiền của người dùng nếu người dùng muốn lấy lại dữ liệu của mình.

Ngày 20/9, các nhà nghiên cứu an ninh mạng tại Info Armor cho biết, họ đã phát hiện ra phần mềm độc hại có tên là RAUM - là một công cụ có trong các diễn đàn chợ đen. Nó lợi dụng hệ thống chia sẻ file torrent - một phương pháp chia sẻ file phổ biến hiện nay liên quan đến vấn đề vi phạm bản quyền, để phát tán các phần mềm độc hại. Những file torrent phổ biến, đặc biệt là các trò chơi, được đóng gói kèm theo các phần mềm độc hại và sau đó được hacker tải lên lên mạng, người dùng sẽ tải các file torrent đó về máy của mình mà không nghi ngờ gì.

Theo các nhà nghiên cứu an ninh mạng, việc sử dụng các file torrent để lây nhiễm các máy tính không phải là mới, nhưng những người tạo ra công cụ RAUM đã sắp xếp toàn bộ các quá trình với một mô hình đó là trả tiền cho mỗi lượt cài đặt (Pay-Per-Install).

Phần mềm RAUM có giao diện bắt mắt, nó có thể theo dõi tình trạng của các file torrent bị nhiễm độc trên các trang web phổ biến về torrent như The Pirate Bay và Extra Torrent, với các torrent mà người dùng tải về thường chứa trong các thư mục với các nội dung vi phạm bản quyền.

Để lây nhiễm thêm nhiều người dùng hơn, những người tạo ra công cụ RAUM cũng đã quan sát và biết được những ai đang tải file lên mạng, sau đó các hacker sẽ chiếm quyền điều khiển của các tài khoản đó và sử dụng những tài khoản đó để phát tán các file torrent bị nhiễm mã độc lên mạng.

Công cụ RAUM đã phát tán và phân phối các dạng phần mềm gián điệp, phần mềm tống tiền (ransomware) như CryptXXX, Trojan Dridex, Pony - có thể đánh cắp thông tin ngân hàng của người dùng như tài khoản, mật khẩu, các thông tin khác…

Theo các nhà nghiên cứu, những người tạo ra công cụ RAUM được cho là một nhóm tội phạm có tổ chức ở Đông Âu được gọi là Black Team. Các công cụ đang được rao bán trên các diễn đàn ngầm chỉ là để mời chào, với các thành viên mới thì quá trình xác minh thông tin khá nghiêm ngặt.

Các nhà nghiên cứu tại Info Armor khuyến cáo mạnh mẽ người dùng phải hết sức thận trọng trước khi truy cập vào các trang chia sẻ torrent hoặc tải về các nội dung kỹ thuật số vi phạm bản quyền, hệ điều hành và các phần mềm kinh doanh./.

Nguồn: NDĐT

Link bài viết: https://nguoilambao.vn/hacker-ban-cong-cu-phat-tan-phan-mem-doc-hai-thong-qua-cac-tap-tin-torrent