"ROOTKIT + TROJAN = NGUY HIỂM GIA TĂNG"

Hãng bảo mật Sana Security hiện đang cảnh báo người dùng về một chủng loại phần mềm độc hại mới được lập trình ra nhằm mục tiêu ăn cắp tên sử dụng và mật khẩu. Phần mềm độc hại "rootkit.hearse" có tính chất nguy hiểm hơn các loại phần mềm độc hại ăn cắp thông tin

Hãng bảo mật Sana Security hiện đang cảnh báo người dùng về một chủng loại phần mềm độc hại mới được lập trình ra nhằm mục tiêu ăn cắp tên sử dụng và mật khẩu. Phần mềm độc hại "rootkit.hearse" có tính chất nguy hiểm hơn các loại phần mềm độc hại ăn cắp thông tin cá nhân trước đây ở điểm nó đã được ứng dụng thêm kĩ thuật "ẩn thân" của các rootkit khiến cho việc phát hiện chúng trở nên vô cùng khó khăn. Tuy nhiên, để có thể thực hiện được chức năng "bẩm sinh", chủng loại phần mềm độc hại này phải đột nhập thành công lên hệ thống của người dùng. Cũng có thể chủng loại phần mềm độc hại này sẽ vẫn sử dụng phương thức lừa người dùng tải về các đoạn mã độc hại hoặc lây nhiễm lên một máy tính thông qua các các loại phần mềm độc hại khác. Một khi đã đột nhập thành công lên hệ thống, "rootkit.hearse" ngay lập tức sẽ gửi các thông tin nhạy cảm về người dùng tới một máy chủ ở Nga. "Rootkit.hearse" có hai bộ phận cấu thành nên: một con trojan giúp nó giao tiếp với máy chủ tại Nga và một phần mềm rootkit giúp nó có thể "ẩn thân" trước các công cụ bảo mật. Hãng bảo mật Sana đã phát hiện ra phần mềm độc hại này được tải xuống kèm theo sâu Win32.Alcra. "Rootkit.hearse" sử dụng kĩ thuật giấu mình tương tự như phần mềm bảo vệ bản quyền XCP "đầy tai tiếng" của Sony BMG Music Entertainment. Phần mềm độc hại này dành phần lớn thời gian của nó "nằm im lìm" dưới nền hệ điều hành; nhưng bất cứ khi nào người dùng truy cập vào một trang web cần có chứng thực thì ngay lập tức nó kích hoạt giao tiếp với máy chủ tại Nga. Nó sẽ tự động đọc các thông tin mật khẩu và tên sử dụng và gửi về máy chủ đó. Tính đến cuối ngày thứ hai vừa qua, theo kết quả thử nghiệm của Sana, chỉ có 5 trong số 24 sản phẩm bảo mật là có khả năng phát hiện "rootkit.hearse". Tính đến ngày hôm qua, máy chủ tại Nga đã chứa tới hơn 35.000 tên đăng nhập và mật khẩu lấy từ hơn 7.000 trang web khác nhau. Sana đã thông báo cho các nhà cung cấp dịch vụ Internet tại Nga xử lý máy chủ lưu trữ này. Tuy nhiên, hãng từ chối tiết lộ thông tin về máy chủ và nhà cung cấp dịch vụ Internet đó.