GIẢI PHÁP NGĂN CHẶN SỬ DỤNG TEENSY – HID TẤN CÔNG MÁY TÍNH

ThS. Phan Trần Điền (*)

Thông tin là một trong những tài sản quan trọng, quý giá đối với mọi tổ chức, doanh nhiệp. Những rủi ro đối với các thông tin như bị lộ, bị thay đổi, bị mất mát, bị từ chối đều ảnh hưởng nghiêm trọng đến hoạt động, đến uy tín, đến chiến lược của tổ chức, doanh nghiệp. Hiện nay, có rất nhiều kỹ thuật tấn công nhằm thay đổi, phá hủy hay mất mát thông tin như: Kỹ thuật keyloger, kỹ thuật tấn công máy tính sử dụng thiết bị HID, kỹ thuật man in middle, kỹ thuật phishing. Kỹ thuật tấn công máy tính sử dụng thiết bị HID được sử dụng phổ biến trong những năm gần đây, với kỹ thuật này, tin tặc sẽ vượt qua cơ chế xác thực của hệ điều hành để thực thi mã độc nhằm chiếm quyền điều khiển máy tính, thay đổi, đánh cắp thông tin từ máy tính. Trong bài viết này, tôi sẽ trình bày giải pháp phòng chống tấn công chiếm quyền điều khiển máy tính bằng kỹ thuật sử dụng dụng Teensy USB – HID.

Thực trạng an toàn thông tin của thiết bị USB

Thiết bị lưu trữ Universal Serial Bus (USB) đã trở thành một tiêu chuẩn sử dụng rộng rãi trong thời đại kỹ thuật số. Các nhà sản xuất thiết bị lưu trữ USB phải tuân thủ các chỉ dẫn trong "phân lớp thiết bị lưu trữ" (USB mass-storage device class) để thông báo đến hệ điều hành về thông tin phần cứng, giúp nhanh chóng xác định và kết nối với nhau thông qua chương trình trình điều khiển thiết bị. Có nhiều tiêu chuẩn được sử dụng rộng rãi trong phân lớp này bao gồm: USB lưu trữ, thẻ nhớ, thiết bị đọc thẻ, máy ảnh kỹ thuật số, máy chơi nhạc MP3/MP4, khung ảnh kỹ thuật số, điện thoại thông minh.

Phương pháp tấn công chủ yếu trên những thiết bị này là có thể chứa những mã độc nhằm lợi dụng sự bất cẩn của người dùng để kích hoạt, đây được xem là dạng tấn công phổ biến và dễ dàng thực hiện tại thời điểm USB mới phổ

(*) *Giảng viên Tin học Khoa Đại Cương, Học viện Cán bộ Thành phố Hồ Chí Minh*

biến. Theo Bkav, virus lây qua USB cũng là một chủ điểm nóng nhất của bức tranh an toàn thông tin (ATTT) trong năm 2016, việc cắt bỏ chức năng Auto Run trong các hệ điều hành của Microsoft, nhưng tỷ lệ USB bị nhiễm virus trong năm 2016 vẫn ở mức rất cao 83% không giảm so với năm 2015.

Trong các phiên bản của hệ điều hành Windows, thì tại phiên bản 95, chức năng Autorun (autorun.info) được các tin tặc triển khai mã độc mà không cần phải kích hoạt thủ công; Windows XP chặn thực thi autorun.inf từ USB, nhưng vẫn cho phép CD/DVD kích hoạt tính năng autorun.inf; Windows Vista đã triển khai chặn autorun.inf trên mọi thiết bị ngoại vi và sự ra đời của cơ chế bảo vệ UAC (User Account Control). Cơ chế bảo vệ UAC vẫn được sử dụng cho những phiên bản Windows 7, Windows 8 và Windows 10 nhằm tăng khả năng kiểm soát việc thực thi mã độc tự động. Nhưng hình thức tấn công sử dụng HID ngày nay đã có thể vượt qua hầu hết các cơ chế kiểm soát an ninh mặc định của hệ điều hành.

Nhận diện phương thức sử dụng Teensy – HID tấn công máy tính

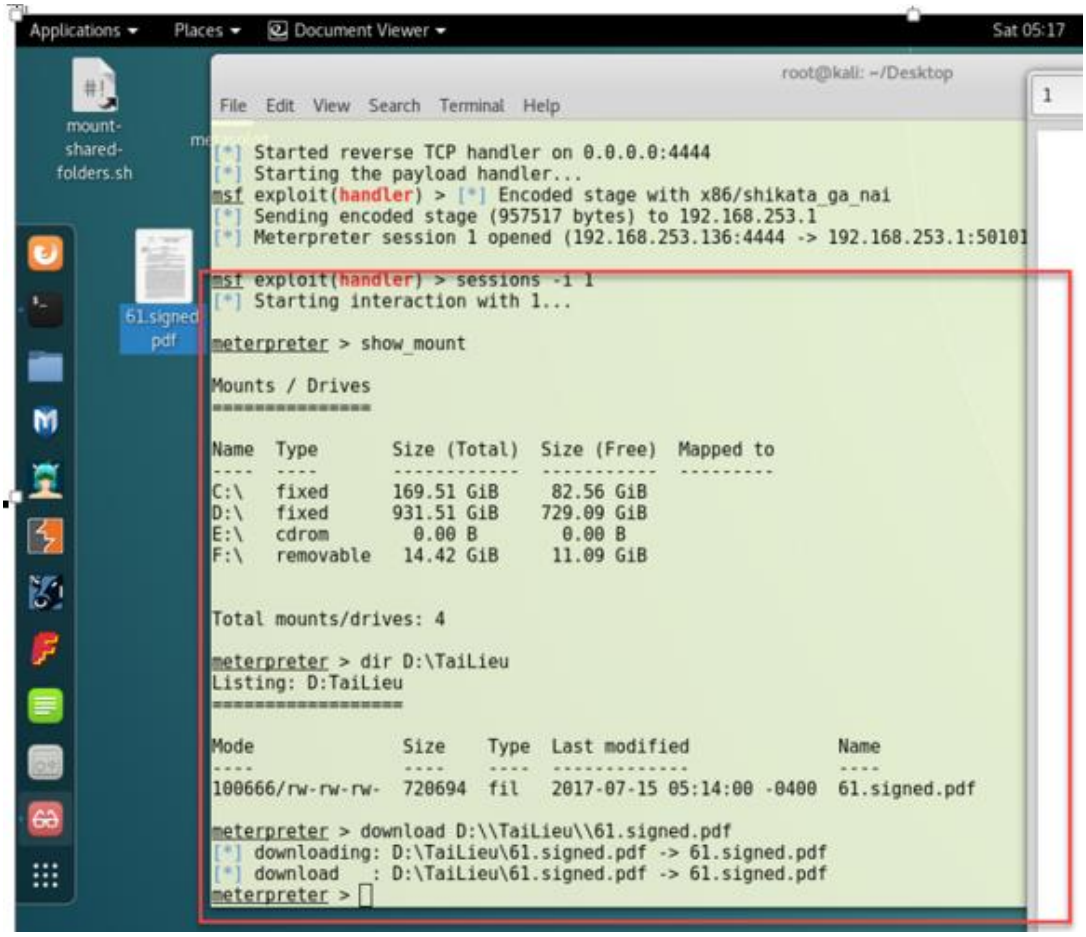
Phương pháp tấn công sử dụng thiết bị HID là lựa chọn hoàn hảo để tin tặc vượt qua các cơ chế kiểm soát của hệ điều hành. Bằng cách lập trình lại vi điều khiển của thiết bị HID, tin tặc có thể giả lập các hành vi của bàn phím, chuột để gởi các thông tin dữ liệu mong muốn đến máy tính hoặc thiết bị kết nối nhằm thực thi mã độc để chiếm quyền điều khiển. Do tính linh động có thể định nghĩa lại vi xử lý, thiết bị HID có thể được chế tạo với nhiều hình dạng khác nhau: Bộ sạc dự phòng, bàn phím, đầu đọc thẻ nhớ… Trên thị trường hiện nay có khá nhiều vi xử lý, mạch tích hợp, thiết bị hỗ trợ HID và người dùng có thể nhanh chóng thay đổi cấu trúc firmware của thiết bị thông qua ngôn ngữ lập trình. Thiết bị tiêu biểu như: Arduino, Espruino, Teensy, USB Rubber Ducky Deluxe,...

Thiết bị Teensy USB

Teensy có thể đóng vai trò là một thiết bị mã độc (lưu trữ các mã dropper trong chính phần cứng thiết bị Teensy), hoặc có thể kết hợp với thẻ nhớ SD để mở rộng vùng lưu trữ dữ liệu (lưu trữ các CVE exploit, 0-day, malware,...);

Metasploit Framework là một môi trường dùng để kiểm tra, tấn công và khai thác lỗi của các service, có thể chạy trên hầu hết các hệ điều hành: Linux, Windows, MacOS.

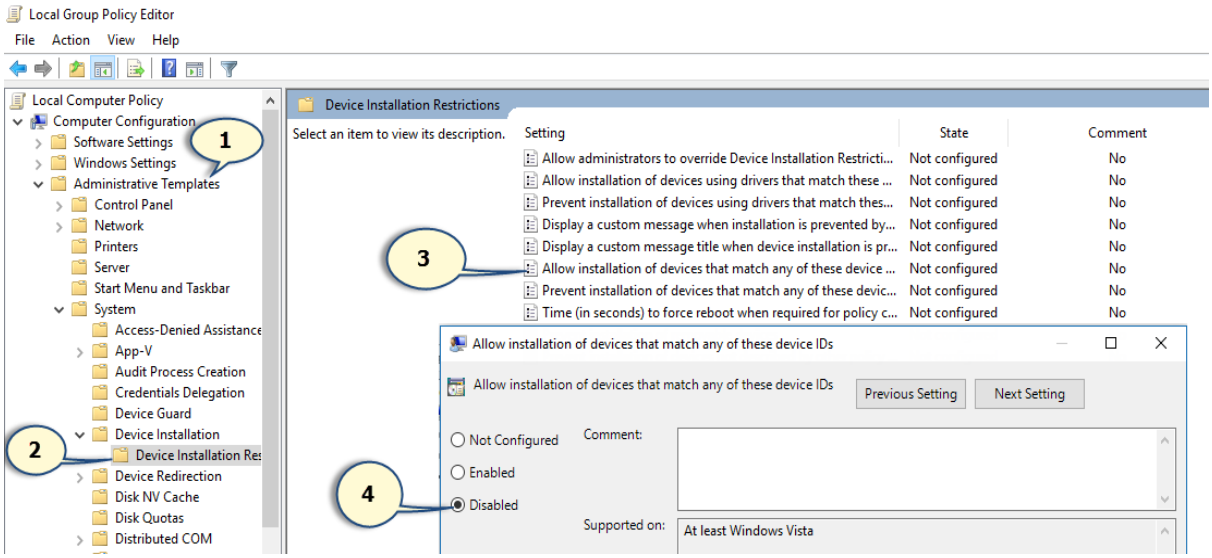
Tin tặc sẽ cài Arduino IDE và thư viện Teensyduino, sau đó tiến hành lập trình và nạp chương trình vào thiết bị qua giao diện Arduino IDE và kích hoạt Metasploit tại máy chủ tin tặc; nạp chương trình Teensy. Sau khi phần cứng Teensy được nạp mã độc, chỉ cần tin tặc cắm thiết bị vào máy tính chạy hệ điều hành Microsoft Windows, người dùng sẽ trở thành nạn nhân và có nguy cơ mất an toàn thông tin, bí mật dữ liệu trong quá trình sử dụng.



Máy tính nạn nhân bị điều khiển và bị lộ tài liệu cá nhân

Giải pháp ngăn chặn việc sử dụng Teensy – HID tấn công máy tính:

Để phát hiện, phòng chống các dạng phần cứng độc hại tấn công máy tính đang sử dụng hệ điều hành Windows, sử dụng dụng chức năng Windows – GPO (Group policy): Chọn *Computer Configuration* trong cửa sổ *Local Group Policy Editor – Administrative Templates – System – Device Intallation Restrictions – Allow installation of devices that match any of these device IDs – Disable*.



Phòng chống các dạng phần cứng độc hại tấn công máy tính sử dụng trên hệ điều hành Windows

Tóm lại, việc kiểm soát chặt chẽ việc sử dụng cổng USB để hạn chế sự lây lan của virus. Người dùng cá nhân cần trang bị phần mềm diệt virus có chức năng giám sát mạng (chức năng tường lửa) để ngăn chặn các kết nối nguy hại. Với các tổ chức, doanh nghiệp cần phải trang bị giải pháp kiểm soát chính sách an ninh đồng bộ, trong đó việc kiểm soát, phân quyền sử dụng cổng USB, tắt chức năng cho phép cài đặt các thiết bị mới để phòng tránh việc tin tặc sử dụng các thiết bị như Teensy – HID kết hợp với Metasploit tấn công chiếm quyền hệ thống máy cá nhân và máy chủ của đơn vị.

Tài liệu tham khảo

[1]. Teensy USB development board, tại : https://www.pjrc.com/teensy/

[2]. Backdoor-peensy,tại:https://github.com/offensive-security/hid-backdoor-peensy

[3]. Arduino IDE, tại: https://www.arduino.cc/en/Main/Software

[4]. Teensyduino, tại: https://www.pjrc.com/teensy/td_download.html

[5]. Quang minh tâm, Tấn công máy tính sử dụng Teensy –HID, tại: http://arduino.vn/bai-viet/970-tan-cong-may-tinh-su-dung-teensy-hid-p1