Tìm hiểu về keylogger là gì?

Keylogger là gì? Nhiều người có thể mơ hồ hiểu rằng keylogger là một thứ gì đó nguy hiểm có thể ghi lại mọi thao tác bấm phím, nhưng không phải ai cũng hiểu rõ về công cụ này.

Chắc hẳn trong chúng ta, nhiều người ta không dưới 1 lần nghe tới khái niệm "keylogger". Tuy có thể cảm nhận mơ hồ rằng đó là thứ nguy hiểm, một công cụ lợi hại có thể giúp kẻ xấu lấy cắp thông tin mà ta nhập vào từ bàn phím. Nhưng liệu bạn đã có thể tự tin nói rằng mình hoàn toàn hiểu đúng về thứ công cụ này? Hãy cùng chúng tôi tìm hiểu về keylogger, mục đích sử dụng của nó, loại thông tin nó thu thập cũng như cách thức nó hoạt động, từ đó rút ra những kinh nghiệm bảo vệ bản thân một cách hiệu quả nhất.

Keylogger là gì?

Keylogger thường là một phần mềm nhỏ gọn – hoặc đôi lúc nguy hiểm hơn thậm chí là một thiết bị phần cứng – với khả năng **ghi lại mọi phím bấm mà người dùng đã nhấn trên bàn phím**. Tổng hợp kết quả của các tổ hợp phím này, kẻ cài đặt keylogger có thể thu được tin nhắn cá nhân, nội dung email, số thẻ tín dụng và dĩ nhiên nguy hiểm nhất là mọi loại mật khẩu của người dùng.

Keylogger thường được sử dụng để làm gì?

Keylogger được sử dụng trong các tổ chức Công nghệ Thông tin (IT) để khắc phục sự cố kỹ thuật với máy tính và mạng lưới kinh doanh. Keylogger cũng có thể được sử dụng bởi một gia đình (hoặc doanh nghiệp) để âm thầm theo dõi việc sử dụng mạng của các thành viên; đôi khi chúng được sử dụng như một phần của tính năng giám sát trẻ em.

Cuối cùng và cũng là mục đích nguy hiểm nhất của keylogger chính là các hacker, người có mưu đồ đen tối có thể cài keylogger trên các máy tính để ăn cắp mật khẩu, thông tin cá nhân, bí mật hoặc thông tin thẻ tín dụng.

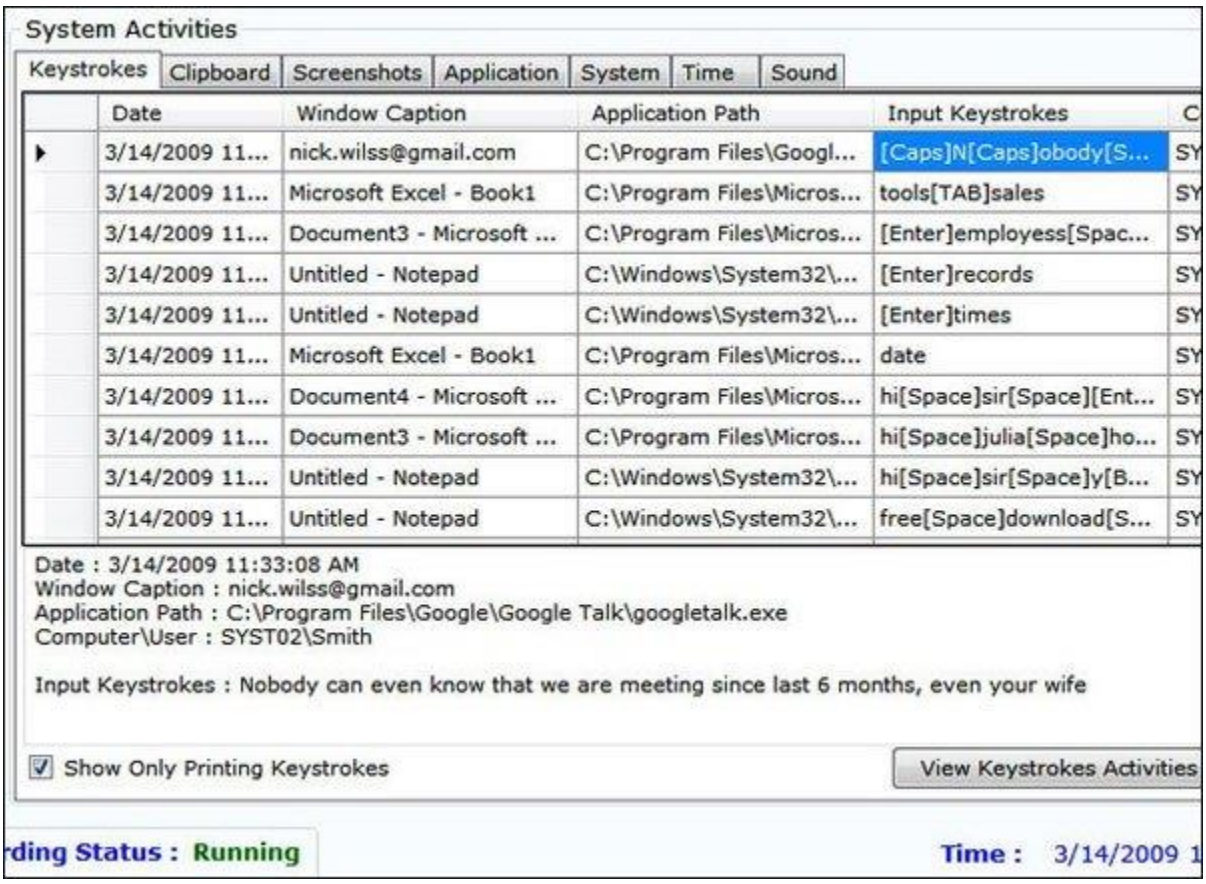
Những thông tin keylogger có thể thu thập?

Tùy từng loại keylogger và mục đích của người tạo ra nó mà nó có những khả năng khác nhau, nhưng khi được gắn trên thiết bị, nó thường có thể thực hiện các thao tác sau:

- Ghi lại bất kỳ mật khẩu nào được người dùng nhập trên thiết bị.
- Chụp ảnh màn hình của thiết bị theo chu kỳ nhất định.
- Khi lại các URL mà người dùng đã vào bằng trình duyệt, thậm chí chụp ảnh các trang web người dùng đã xem.
- Ghi lại danh sách các ứng dụng người dùng chạy trên thiết bị.
- Chụp bản ghi của tất cả tin nhắn tức thời (Zalo, Facebook Messenger, Skype, Viber,...)
- Chụp bản sao email đã gửi
- Tự động gửi báo cáo chứa các bản ghi được lưu trữ và gửi email đến một địa điểm từ xa thông qua email, FTP, HTTP.

Hầu hết các keylogger không chỉ ghi lại những thao tác bàn phím của người dùng mà còn có thể chụp màn hình máy tính. Keylogger có thể lưu trữ dữ liệu mà nó thu thập được ngay trên ổ cứng của người dùng hoặc tự đồng truyền dữ liệu qua mạng tới máy tính từ xa hoặc Web Server.

Keylogger xâm nhập vào máy theo cách nào?



Trong đa số trường hợp, keylogger được **các malware cài đặt một cách âm thầm lên máy người dùng** sau khi thâm nhập thành công. Một số trường hợp khác có phần ít gặp hơn là khi cha mẹ muốn quản lý truy cập của con cái, khi các quản lý của một công ty muốn kiểm tra thái độ làm việc của nhân công hay… các cặp đôi muốn theo dõi nhau. Ở Việt Nam, đôi lúc ta cũng nghe được chuyện keylogger nằm trong các máy của hàng net – không phải do máy bị nhiễm malware mà do một kẻ nào đó táy máy muốn "thử tay nghề" của mình, thậm chí có người còn cho rằng chính các chủ quán là người chỉ đạo việc này. Thực hư của các lời đồn cũng như tính hợp pháp của các trường hợp động chạm đến riêng tư cá nhân của từng người – kể cả khi cha mẹ muốn theo dõi con cái là chuyện vẫn còn nằm trong vòng tranh cãi. Nhưng nhu cầu quản lý nhân viên của các tổ chức lớn thông qua keylogger là có thật, và người ta thậm chí đã có những dòng sản phẩm phần cứng chuyên dùng cho công việc này.

Như đã nói ở trên, đa số keylogger trên các máy tính phổ thông được phát tán qua các malware. Nếu máy tính của người dùng đã bị thâm nhập, đoạn mã độc này có thể mang sẵn trong mình chức năng của một phần mềm keylogger nhỏ gọn – hoặc

nó có thể hoạt động như một Trojan, tiến hành tải về và cài đặt gói keylogger một cách âm thầm, thậm chí là kèm theo nhiều phần mềm độc hại khác. Thường thì các malware cũng sẽ tự động thiết lập một kênh để gửi thông tin mà keylogger thu được về cho "chủ nhân". Có thể nói keylogger là một trong những công cụ được tin tặc ưa chuộng nhất bởi chúng có thể thu được mọi loại thông tin của người dùng bằng phương pháp này.

Ngoài kênh xâm nhập bằng malware, đa số các trường hợp máy nhiễm keylogger còn lại xuất phát từ người thân của chúng ta. Hai đối tượng dễ có liên quan nhất, như đã nêu từ trước, dĩ nhiên là các bậc phụ huynh và... người yêu (hoặc vợ/chồng). Các bậc cha mẹ cảm thấy cần phải kiểm soát kĩ lượng việc truy cập thế giới Internet rộng lớn của con mình thường sử dụng các gói phần mềm quản lý (parental controls), trong đó thường không khó để tìm ra chức năng tương tự keyloggers. Và dĩ nhiên trong thế giới mạng ngày nay, một cô nàng hay ghen với một chút vốn tiếng Anh sẽ chỉ mất chưa đầy 30' để Google ra một bộ cài keylogger (hoặc các phần mềm thậm chí đa chức năng hơn) nhằm theo dõi xem bạn có lén lút "ăn phở" ở ngoài không.

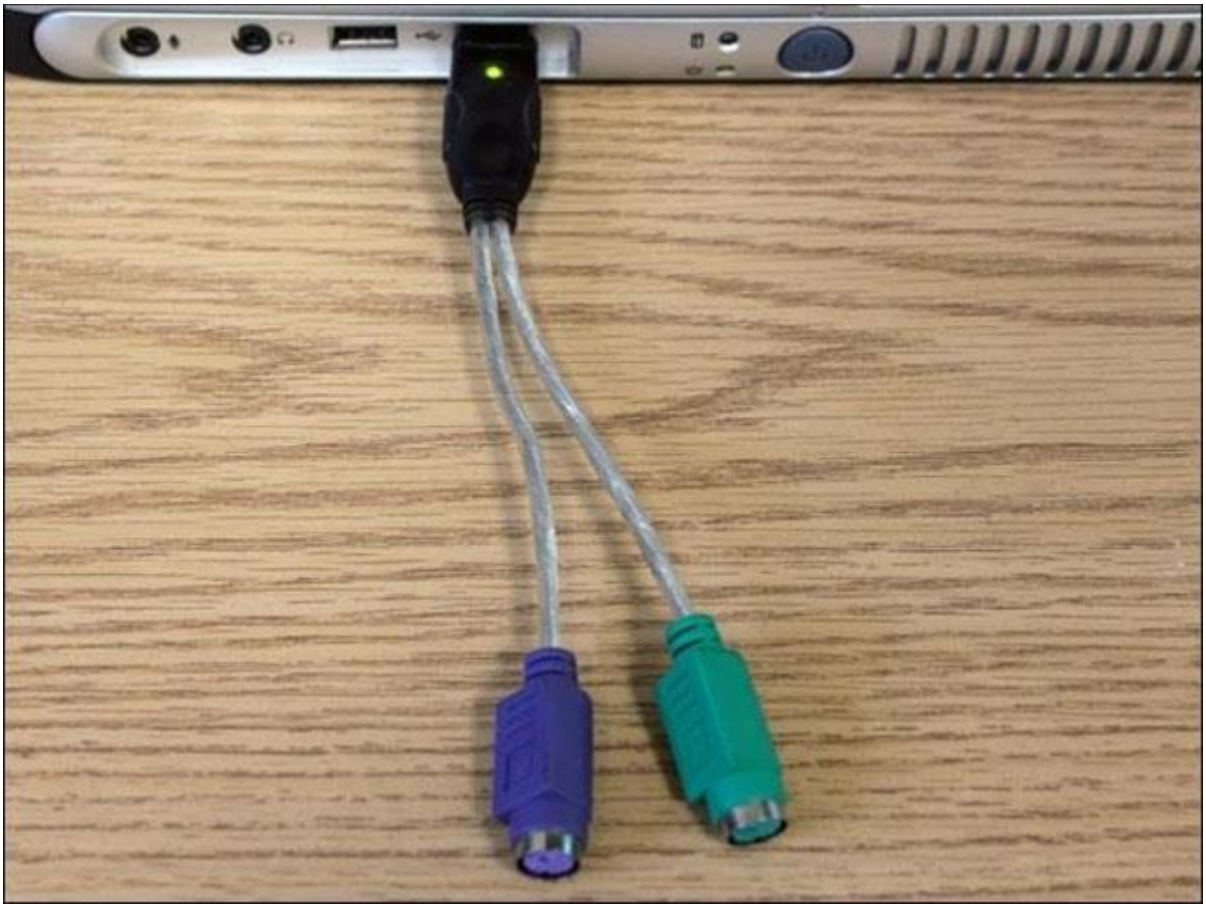
Còn trong trường hợp các ông chủ chỉ đạo cài đặt keylogger trên máy của nhân viên, cần nhớ rằng việc phân tích kết quả mà keylogger thu được, đặc biệt là với số lượng lớn máy không phải là việc tốn ít công sức và tài nguyên. Trong đa số trường hợp nếu phát hiện mình đang trong "tầm ngắm", hãy tự kiểm tra lại xem mình có làm gì để bị đặt vào diện "đối tượng tình nghi" để lộ thông tin của công ty hay không trước. Các bộ luật liên quan đến vấn đề theo dõi này cũng thay đổi tùy thuộc theo quốc gia và vùng địa lý. Đồng thời một số công ty cũng yêu cầu nhân viên không làm việc cá nhân trong môi trường công sở, vì vậy việc theo dõi như vậy vẫn được một số người cho là hợp pháp và hợp lý – bởi dù sao thì nếu nhập thông tin cá nhân trên các máy này đồng nghĩa với việc bản thân nhân viên đó đã vi phạm quy định, không thể trách ai khác được.

Phần mềm Keylogger

Đây là những keylogger được cấu hình trong các chương trình chạy trên máy tính của bạn. Các keylogger này được cài đặt trên máy tính của bạn bởi các hacker và chạy trên nền background, trong một số trường hợp người dùng khó có thể mà phát hiện được.

Loại keylogger này được sử dụng để chuyển tiếp dữ liệu tới hacker. Chúng có thể làm "tê liệt" hệ thống của bạn.

Phần cứng keylogger



Với tiến bộ của công nghệ ngày nay, việc tạo ra một keylogger dưới dạng thiết bị phần cứng không còn là điều gì quá khó khăn. Như chúng ta đều biết, bàn phím PC thường được nối với case qua cáp nối sử dụng cổng USB (hoặc một số mẫu vẫn sử dụng cổng PS2). Việc kết nối các phần cứng keylogger chuyên dụng chỉ đơn giản là tháo kết nối của bàn phím tới case, cắm vào thiết bị keylogger nhỏ gọn. Thiết bị này dĩ nhiên sau đó được nối tiếp vào case để bảo đảm người dùng vẫn nhập dữ liệu được một cách bình thường mà không mảy may phát hiện, đặc biệt là trong một số môi trường công sở mà nơi đặt case thường được đóng kín và đôi lúc chỉ có nhân viên IT mới có chìa khóa tiếp cận. Ngay cả trong quán net, hay với những người dùng bất cẩn không bao giờ động tới case nằm bụi bặm dưới gầm bàn của mình, cách này cũng vẫn rất hiệu quả. Với cách làm này, không phần mềm bảo mật được cài đặt trên máy có thể giúp chúng ta phát hiện ra rằng các dữ liệu nhập vào

từ bàn phím đang âm thầm được ghi lại, bởi thiết bị này không thông báo gì với hệ điều hành về sự hiện diện của nó.

Tuy thường không có lợi thế như các phần mềm được malware cài đặt là có thể gửi dữ liệu thu được qua mạng. Nhưng người lắp đặt thiết bị keylogger chỉ cần quay lại sao vài ngày, rút thiết bị ra và cắm bàn phím lại như cũ là đã có trong tay một lượng dữ liệu tương đối lớn của người sử dụng. Quan trọng nhất vẫn là việc nó không để lại bất kì dấu vết "mềm" nào để mắt các phần mềm bảo mật, phân tích kết nối… có thể phát hiện ra.

Đôi lúc, các thiết bị này còn có thể được ngụy trang dưới dạng adapter trông có vẻ rất "hiền lành" như trong bức hình phía trên. Hay xuất hiện trong USB hoặc các thiết bị ổ cứng di động khác. Trong hầu hết các trường hợp, các keylogger này được nhúng ở mặt sau CPU để ghi lại thao tác bàn phím của người dùng.

Cách thức hoạt động của keylogger

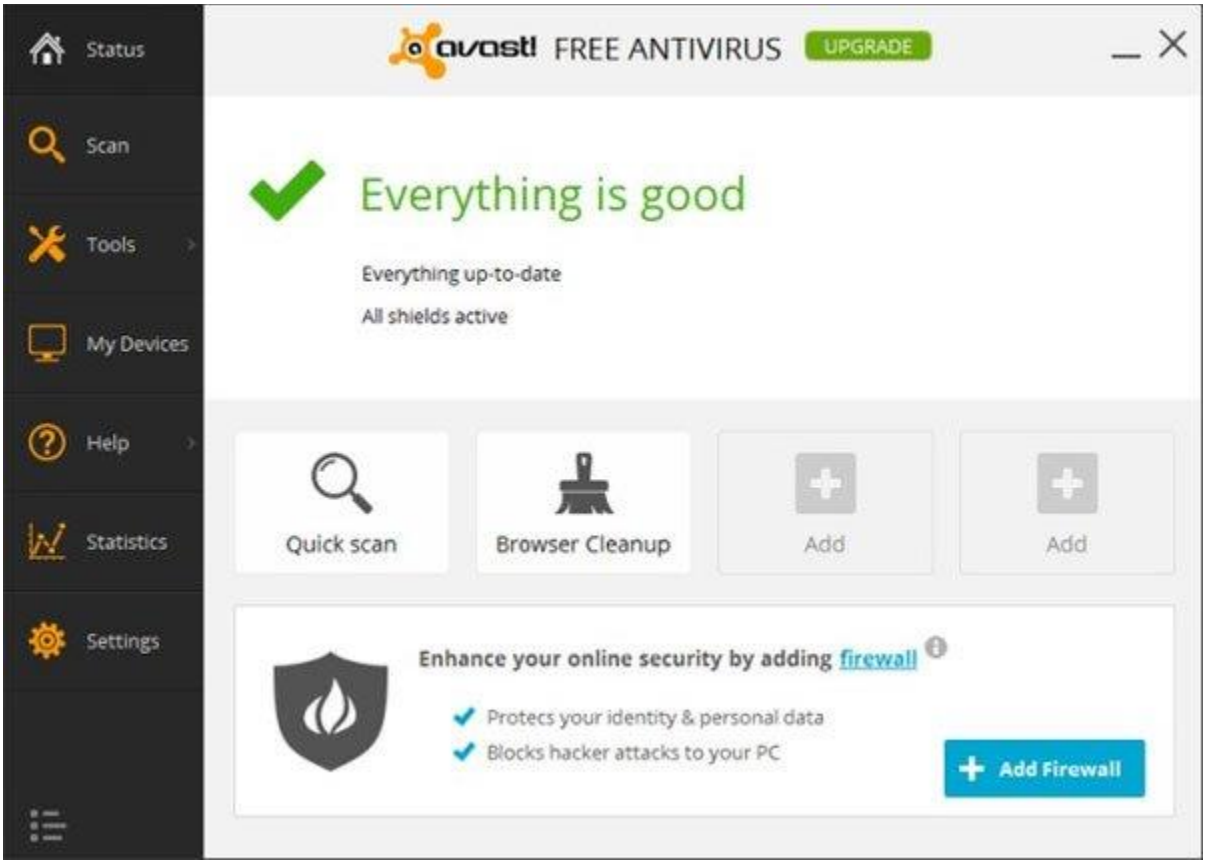
Keylogger dưới dạng phần mềm thường chạy ngầm trên máy, ghi lại mọi phím bấm mà người dùng nhập vào. Đôi lúc để tránh việc gửi dữ liệu thường xuyên khiến việc theo dõi bị người dùng "chú ý", các gói phần mềm này có thể được thiết kế để chỉ gửi đi các chuỗi dữ liệu có vẻ hữu dụng – chẳng hạn như một chuỗi số "có vẻ" giống mã thẻ tín dụng.

Để tăng tính hiệu quả, keylogger cũng thường được kết hợp với một số loại phần mềm theo dõi khác, nhờ vậy kẻ xâm nhập có thể phân biệt được các thông tin mà người dùng nhập vào khi chat chit vô nghĩa với các thông tin nhập vào khi đang đăng nhập vào tài khoản ngân hàng trực tuyến. Các chuỗi kí tự đầu tiên người dùng nhập vào sau khi khởi động một **chương trình chat, email client hay game online cũng rất quan trọng** – bởi đây thường là chuỗi username và password dùng để đăng nhập vào tài khoản của dịch vụ đó.

Với những trường hợp cần được "chăm sóc" tỉ mỉ hơn, kẻ cài đặt keylogger thường sẽ phải sử dụng công cụ để quét qua toàn bộ file log ghi lại tất cả những gì người dùng đã nhập vào trong suốt thời gian bị theo dõi, từ đó lọc ra cả những thông tin như nội dung tìm kiếm Google, comment trong một topic… bậy bạ nào đó trên mạng. Thường thì các gói phần mềm theo dõi cung cấp cho các bậc phụ huynh và các công sở còn được tích hợp cả tiện ích chụp ảnh màn hình. Từ đó cung cấp đầy

đủ thông tin và bằng chứng về những gì mà "nạn nhân" đã làm trong suốt quá trình sử dụng máy.

Bảo vệ mình trước keylogger



Về cốt lõi, phần mềm keylogger vẫn luôn được xếp vào dạng mã độc – malware. Vì vậy ta có thể phát hiện keylogger trên máy bằng các công cụ quét thường dùng. Quan trọng nhất là hãy chọn đúng phần mềm bảo mật – không cần thiết phải mạnh mẽ và đắt tiền, chỉ cần có tên tuổi và danh tiếng rõ ràng. Avast, AVG, Avira đều có các giải pháp miễn phí và hiệu quả cho người dùng phổ thông. Nếu thiếu cẩn trọng, rất có thể phần mềm gán "anti-virus" hay "anti-malware" mà bạn tải bừa từ một nguồn nào đó trên mạng lại chính là thủ phạm cài đặt keylogger lên máy của bạn, hoặc nhẹ nhàng hơn thì sẽ kéo theo vô vàn bloatware – các phần mềm không mong muốn - cũng như các quảng cáo khó chịu lên máy.

Nếu thật sự lo lắng và không chắc về sự tồn tại của keylogger hay xa hơn là các phần mềm quản lý do người khác cài đặt lên máy mình, tốt nhất là bạn hãy luôn tận dụng chức năng bàn phím ảo sẵn có trên các dịch vụ của ngân hàng, kênh thanh

toán trực tuyến hay các game online. Đừng để một ngày đẹp trời sau khi đăng nhập vào game thì bi phẫn nhận ra nhân vật của mình đã bị "lột trần", trong khi thủ phạm không phải ai xa lạ mà chính là các bậc... phụ huynh.