MODULE VII: Xử lý các nguy cơ nội bộ

Tin tức: Các cuộc tấn công mã độc trong nội bộ gia tăng

Viết bởi: Maggie Shiels

Phóng viên công nghệ tại đài BBC, Silicon Valley

Công ty phần mềm lớn nhất trên thế giới đã cảnh cáo các công tu về nguy cơ gia tăng các cuộc tấn công bảo mật "nội bộ" bởi những công nhân bất mãn hoặc bị sa thải.

Microft cho biết những vi phạm trên đang gia tang và sẽ trở nên tồi tệ hơn trong thời kỳ suy thoái.

Doug Leland cho biết : "Với 1,5 triệu người được dự đoán mất việc làm ở riêng Mỹ, nguy cơ xảy ra các cuộc tấn công nội bộ sẽ tăng lên".

"Đây là một trong nhưng mối đe dọa lớn nhất mà các công ty phải đối mặt", ông nói.

Là người phụ trách một bộ phận mới được thành lập Identity and Security của công ty, Lelan nói với đài BBC rằng tác động của các cuộc tấn công như vậy có thể lan rộng hơn.

"Kẻ gây nên các cuộc tấn công nội gián có thể được coi là những kẻ kiêu ngạo nhất vì họ có quyền truy cập, cà dễ dàng tác động đến tài sản của công ty." ông Leland nói.

Thiệt hại hàng nghìn đô

Một nghiên cứu vào năm ngoài của Verizon ở Mũ cho thấy các vị phạm nội bộ chiếm đến 18% các cuộc tấn công mạng gây ra bởi tin tặc từ bên ngoài, các đặc vụ chính phủ hoặc các công ty đối địch.

Báo cáo cho thấy 230 triệu hồ sơ trong 4 năm liên quan đến các lĩnh vực tài chính, công nghệ, bán lẻ và thực phẩm.

Một nghiên cứu của McAfee đã đưa ra tổng thiệt hại kinh tế toàn cầu do đánh cắp dữ liệu và vi phạm bảo mật do tội phạm có tổ chức, tin tặc và nội gián lên tới 1 ngìn tỉ USD vào năm ngoái.

2

Mục tiêu module

Module này sẽ giúp bạn làm quen với:

- Nguy cơ "nội gián"
- Phân tích chuyên sâu của một cuộc tấn công "nội gián"
- Phát hiện tấn công "nội gián"
- Phản ứng với tấn công "nội gián"
- Kiểm soát tấn công "nội gián"
- Hướng dẫn để phát hiện và kiểm soát tấn công "nội gián"

3

Nguy cơ "nội gián"

"Nội gián" với các quyền được cấp của họ có thể sử dụng không đúng ảnh hưởng trực tiếp đến tính bảo mật, tính toàn vẹn và tính khả dụng của hệ thống thông tin

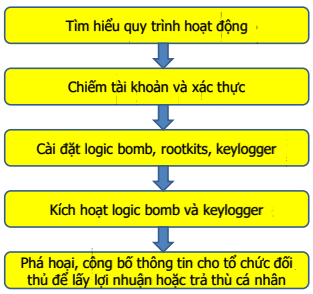
"Nội gián" có thể là nhân viên hiện tại, người quản trị hệ thống, nhân viên tuyển dụng, người liên lạc, đối tác ...

"Nội gián" thực hiện những hành vi lên mạng của tổ chức, hệ thống và cả cơ sở dư liệu

Những hành vi đó ảnh hưởng đến việc điều hành công việc và gây hại cho danh tiếng cũng như lợi nhuận của tổ chức.

4

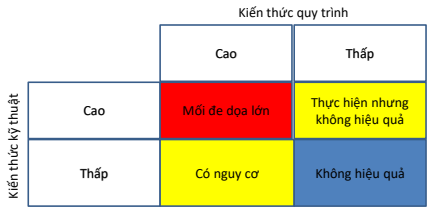
Phân tích chuyên sâu của một cuộc tấn công "nội gián"



5

Ma trận mối nguy "nội gián"

Nếu kẻ tấn công có kiến thức về kỹ thuật với kiến thức về quy trình, thì có nguy cơ tấn công "nội gián" là cao nhất



Nguồn: GartnerGroup Report 5605

6

Phát hiện nguy cơ "nội gián"

Các mối đe dọa "nội gián" có thể được phát hiện bằng cách quan sát các hành vi liên quan đến các những người trong cuộc chẳng hạn như xung đột với người giám sát và đồng nghiệp, suy giảm hiệu suất, đi học muộn hoặc vắng mặt không rõ nguyên nhân

Các mối đe dọa nội bộ có thể được xác định bằng cách kiểm tra nhật ký sự kiện hệ thống bao gồm cơ sở dữ liệu nhật ký, nhật ký email, nhật ký ứng dụng, nhật ký truy cập tệp và nhật ký truy cập từ xa

Các ứng dụng như tường lửa, bộ định tuyến và hệ thống phát hiện xâm nhập có thể được sử dụng để xác định các mối đe dọa nội bộ

Các kỹ thuật được sử dụng để phát hiện các mối đe dọa nội gián

- Tương quan
- Phát hiện sự bất thường
- Khám phá mẫu

7

Phản hồi về các mối đe dọa nội bộ

Phản ứng phụ thuộc vào bản chất của các mối đe dọa nội bộ và chính sách của tổ chức

Phản hồi có thể được tự động hóa hoặc cần sự tham gia của con người

Các kỹ thuật được sử dụng để đối phó với mối đe dọa nội gián bao gồm:

- Đặt người dùng nguy hiểm vào mạng cách ly để cuộc tấn công không thể lây lan
- Ngăn người dùng nguy hiểm truy cập thông tin nhạy cảm
- Tắt hệ thống máy tính khỏi Internet
- Chặn các tài khoản người dùng độc hại và hạn chế họ xâm nhập vào các khu vực kiểm soát truy cập

8

Kế hoạch ứng phó về các mối đe dọa nội bộ

Kế hoạch ứng phó về các mối đe dọa nội bộ giúp làm giảm thiểu thiệt hại gây ra bởi những người dùng nguy hiểm trong nội bộ

Các tổ chức phải đảm bảo rằng thủ phạm nội gián không được đưa vào nhóm ứng phó hoặc không biết về tiến trình kế hoạch ứng phó

Các tổ chức nên xem xét kỹ khi phân các quyền của mọi nhân viên hoặc người dùng trong khi phát triển kế hoạch ứng phó sự cố

Kế hoạch phải mô tả quá trình phải tuân theo và trách nhiệm của các thành viên tham gia vào đội ứng phó

Tổ chức không nên chia sẻ hoặc cung cấp thông tin chi tiết về vụ việc của người trong kế hoạch ứng phó với tất cả nhân viên

9

Hướng dẫn phát hiện và ngăn ngừa Mối đe dọa từ người trong cuộc: An ninh mạng

Mạng máy tính phải được bảo mật bằng cách định cấu hình tường lửa và giám sát việc gửi đi lưu lượng truy cập vào các dịch vụ HTTP và HTTPS

Tạo các quy tắc để giám việc chuyển tệp ra bên ngoài cho một nhóm người dùng được ủy quyền và hệ thống

Ngăn chia sẻ tệp, nhắn tin tức thì và các tính năng khác giữa các nhân viên cho phép truy cập trái phép vào mạng công ty

Quét tất cả các thư đi và đến để tìm thông tin nhạy cảm và mã độc hại

Thiết lập các chính sách mật khẩu nghiêm ngặt

Thực hiện các chính sách và thủ tục quản lý tài khoản

10

Hướng dẫn phát hiện và ngăn ngừa Mối đe dọa từ người trong cuộc: Kiểm soát truy cập

Các đặc quyền truy cập phải được bật cho nhân viên hoặc người dùng dựa trên thực hiện thường xuyên các vai trò công việc của họ

Các yêu cầu truy cập được cấp cho người dùng phải được lập thành văn bản và kiểm tra bởi một người giám sát

Nhân viên nên xin phép chủ sở hữu dữ liệu trước khi truy cập các hệ thống nhạy cảm

Thiết lập các kiểm soát thay đổi trên hệ thống của người dùng

Khi người lao động nghỉ việc, người sử dụng lao động phải vô hiệu hóa tất cả các quyền truy cập vào các vị trí thực tế, mạng, hệ thống, ứng dụng và dữ liệu

11

Hướng dẫn phát hiện và ngăn ngừa Mối đe dọa từ người trong cuộc: Chương trình nâng cao nhận thức về bảo mật

Xác định và báo cáo hành vi độc hại của người dung nội bộ

Kiểm tra các chính sách và kiểm soát của tổ chức

Thực hiện các biện pháp bảo vệ hệ thống quản trị thích hợp cho các máy chủ

Thống nhất các chính sách và kiểm soát bảo mật đã xác định

Thống nhất các định nghĩa bảo mật và chính sách kiểm soát

Thực hiện sao lưu an toàn và các phương pháp khôi phục để đảm bảo dữ liệu

12

Hướng dẫn phát hiện và ngăn ngừa Mối đe dọa từ người trong cuộc: Quản trị viên và Người dùng Đặc quyền

- Vô hiệu hóa các tài khoản quản trị mặc định
- Đảm bảo rằng quản trị viên sử dụng tài khoản duy nhất trong quá trình cài đặt
- Triển khai kỹ thuật chống chối bỏ để xem tất cả các hành động được thực hiện bởi quản trị viên và có đặc quyền người dùng
- Giám sát hoạt động của quản trị viên hệ thống và người dùng đặc quyền có quyền truy cập thông tin nhạy cảm
- Sử dụng các phương pháp mã hóa để hạn chế quản trị viên và những người dùng có đặc quyền truy cập các băng sao lưu và thông tin nhạy cảm

13

Hướng dẫn phát hiện và ngăn ngừa Mối đe dọa từ người trong cuộc: Sao lưu

- Các tổ chức nên thực hiện sao lưu và phục hồi an toàn các quy trình để tiếp tục hoạt động kinh doanh khi hệ thống bị xâm phạm
- Thường xuyên sao lưu và kiểm tra tính toàn vẹn và tính khả dụng
- Bảo vệ phương tiện sao lưu và nội dung của nó khỏi bị thay đổi, đánh cắp, hoặc phá hủy
- Thực hiện tách biệt các nhiệm vụ và cấu hình quy trình quản lý để thực hiện sao lưu trên máy tính hệ thống, mạng và cơ sở dữ liệu
- Thực hiện các chính sách sao lưu để đảm bảo quá trình sao lưu và phương tiện truyền thông

14

Hướng dẫn phát hiện và ngăn ngừa Mối đe dọa từ người trong cuộc: Điều tra dấu vết và nhật ký giám sát

- Thực thi các chính sách và thủ tục về tài khoản và mật khẩu để xác định các hành động trực tuyến thực hiện bởi người dùng nội bộ
- Quá trình ghi nhật ký, giám sát và đánh giá định kỳ giúp tổ chức xác định và điều tra các hành động nội gián đáng ngờ
- Các quá trình điều tra dấu vết phải được định cấu hình cho các thiết bị mạng, hệ điều hành, thương mại phần mềm và các ứng dụng tùy chỉnh
- Kiểm toán viên nên xem xét và kiểm tra những thay đổi được thực hiện trên các tài sản trọng yếu bất kỳ của tổ chức
- Bảo vệ các tệp kiểm tra thông qua quyền đối với tệp và lưu trữ tệp trong máy chủ lưu trữ trung tâm để tránh thay đổi
- Triển khai phần mềm phát hiện xâm nhập và sửa đổi tệp để phát hiện và giám sát hoạt động đáng ngờ trên dữ liệu nhạy cảm

15

Tools

- Công cụ giám sát nhân viên

16

Activity Monitor

- Activity Monitor là một phần mềm giám sát máy tính và trình ghi khóa
- Nó cho phép bạn theo dõi bất kỳ mạng Lan nào, cung cấp cho bạn thông tin chi tiết về hoạt động mạng của người dùng

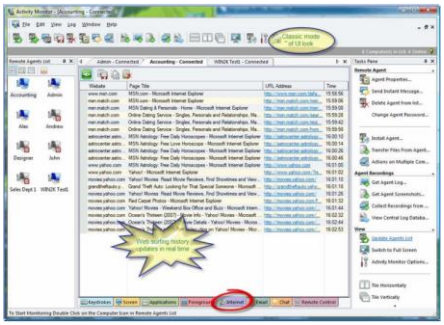
Đặc trưng:
- Xem trực tiếp máy tính để bàn từ xa
- Giám sát việc sử dụng Internet dễ dàng
- Giám sát việc sử dụng phần mềm
- Ghi lại nhật ký hoạt động cho tất cả các nơi làm việc ở một vị trí tập trung trên mainmáy tính có cài đặt Activity Monitor
- Lưu trữ toàn bộ lịch sử liên lạc cho mọi người dùng
- Theo dõi bất kỳ lần nhấn phím nào của người dùng trên màn hình của bạn ở chế độ thời gian thực

17

Activity Monitor: Screenshot 1

18

Activity Monitor: Screenshot 2



19

Net Spy Pro

Net Spy Pro là phần mềm giám sát mạng của nhân viên và sinh viên

Nó cho phép bạn giám sát tất cả hoạt động của người dùng trên mạng của bạn trong thời gian thực từmáy trạm của riêng bạn

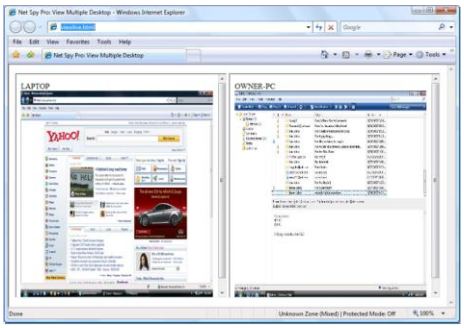
20

Net Spy Pro

Tính năng:
• Cho phép quản trị viên xem ảnh chụp màn hình thực tế của một, một số hoặc tất cảmáy trạm ngay lập tức
• Hiển thị danh sách các mục yêu thích trên Trình duyệt Internet Explorer của người dùng vớingười quản lý
• Hiển thị cho bạn danh sách tất cả các tệp trong lịch sử tạm thời (bộ nhớ cache) của InternetTrình duyệt Explorer
• Cho phép quản trị viên xem tất cả các cổng đang mở trên máy trạm
• Hiển thị danh sách đầy đủ các quy trình và dịch vụ đang chạy trên máy từ xa chongười quản lý
• Hiển thị danh sách các tài liệu gần đây do người dùng mở cho quản trị viên

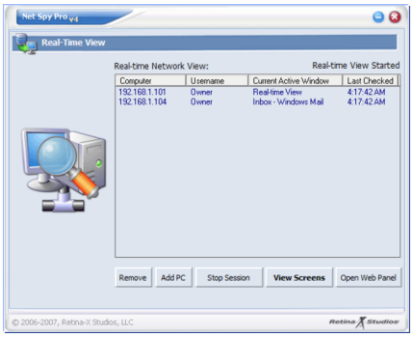
21

Net Spy Pro: Screenshot 1



22

Net Spy Pro: Screenshot 2



23

Spector Pro

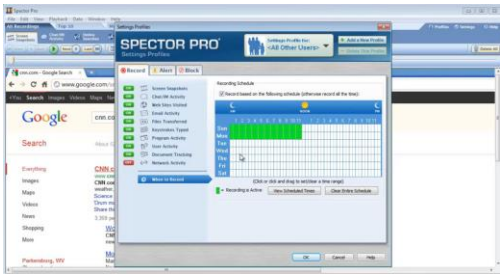
Spector Pro là công cụ giám sát và ghi lại chi tiết hoạt động internet của máy tính

Các nội dung được ghi lại bao gồm:

- Tìm kiếm trực tuyến, từ khoá, dữ liệu nhập vào
- Hoạt động người dùng, mail, mạng xã hội
- Trang web được tìm kiếm, ghé thăm
- Tệp tin trao đổi
- Báo cáo tóm tắt về hệ thống

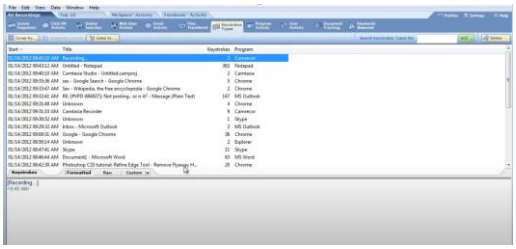
24

Spector Pro: Screenshot 1



25

Spector Pro: Screenshot 2



26

SpyAgent

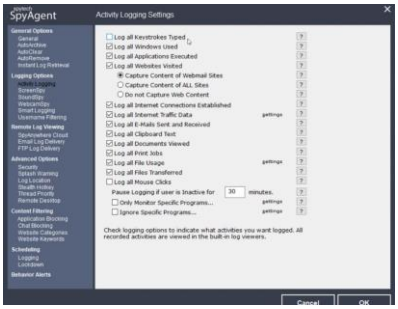
Spytech SpyAngent là phần mềm máy tính cho phép theo dõi , giám sát người dùng trong máy tính

Các nội dung được ghi lại bao gồm:

- Hoạt động đăng nhập, nhật ký đăng nhập
- Hoạt động người dùng nhắn tin qua internet, gửi nhận mail
- Giám sát hoạt động của ứng dụng, trang web
- Ghi màn hình, ghi dữ liệu mạng
- Các tệp tin tải về và gửi đi

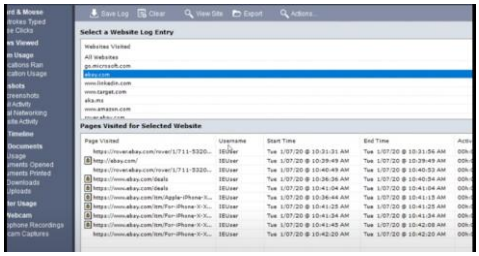
27

SpyAgent: Screenshot 1



28

SpyAgent: Screenshot 1



29

Handy Keylogger

Spector Pro là công cụ theo dõi, chụp lại màn hình và gửi thông tin về hệ thống tới e-mail của người dùng

Các nội dung được giám sát bao gồm:

- Tất cả hoạt động nhập vào từ bàn phím
- Ghi lại các tài khoản, mật khẩu, tin nhắn
- Trang web được tìm kiếm, ghé thăm
- Các sự kiện, cuộc trò chuyện, mail

30

Handy Keylogger: Screenshot 1

31

Handy Keylogger: Screenshot 1

32

Chống Keylogger

Anti-keylogger là một sản phẩm chống keylogging chuyên dụng cho Microsoft Windows

Nó bảo vệ máy tính chống lại các chương trình và mô-đun ăn cắp thông tin

33

Chống Keylogger

Đặc trưng:

- Ngăn chặn danh tính trực tuyến thef
- Ngăn chặn gian lận ngân hàng qua Internet
- Bảo mật thông tin liên lạc qua email, nhắn tin nhanh và trò chuyện
- Loại bỏ rò rỉ thông tin bí mật hoặc độc quyền
- Giữ an toàn cho tên người dùng, mật khẩu, mã PIN, v.v.
- Giảm vi phạm bảo mật
- Thực thi Chính sách sử dụng được chấp nhận trên máy tính và Internet (AUP)
- Tắt phần mềm gián điệp của đối thủ cạnh tranh của bạn

34

Chống Keylogger

35

Gián điệp thực tế

Actual Spy là một keylogger cho phép bạn tìm hiểu những gì người dùng khác làm trên máy tính của bạn khi bạn vắng mặt

Nó có khả năng bắt tất cả các lần gõ phím, chụp màn hình, ghi nhật ký các chương trình đang được chạy và đóng, giám sát nội dung khay nhớ tạm

36

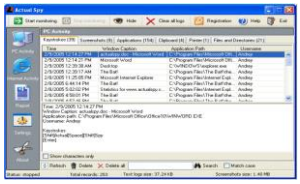
Gián điệp thực tế

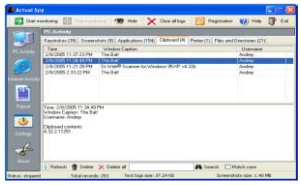
Đặc trưng:

- Ghi lại tất cả các lần gõ phím
- Tạo ảnh chụp màn hình trong khoảng thời gian được chỉ định
- Lưu các ứng dụng đang chạy và đóng
- Xem nội dung khay nhớ tạm
- Ghi lại tất cả hoạt động in
- Ghi lại các thay đổi trên đĩa
- Ghi lại kết nối internet
- Ghi lại tất cả các trang web đã truy cập

37

Gián điệp thực tế





38

IamBigBrother

- IamBigBrother là một phần mềm giám sát internet cho cả gia đình và kinh doanh
- Nó chạy ở chế độ ẩn mà người dùng máy tính không phát hiện được
- Nó ghi lại tất cả các hoạt động internet cho nhiều chương trình bao gồm cả nước Mỹ, MSN, Outlook Express, v.v.

39

IamBigBrother

Đặc trưng:

- Trò chuyện và ghi âm tin nhắn tức thì
- Ghi email
- Trang web đã xem
- Ghi lại tổ hợp phím
- Chụp màn hình

40

IamBigBrother

41

007 Spy Software

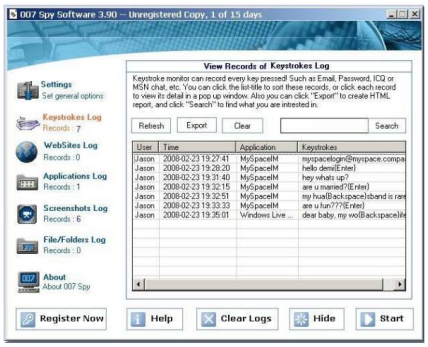
007 Spy Software là phần mềm giám sát máy tính cho phép bạn bí mật ghi lại tất cả các hoạt động của máy tính và chụp nhanh màn hình tại nơi thiết lập khoảng thời gian

Tính năng:

- Khả năng ghi đè các chương trình Chống gián điệp như Nhận biết quảng cáo
- Xem nhật ký từ xa bằng các trình duyệt yêu thích của bạn từ mọi nơi mọi lúc
- Hỗ trợ bộ lọc người dùng để theo dõi những người dùng cụ thể
- Xem tất cả Nhật ký của người dùng với một lần đăng nhập
- Chụp màn hình ở tốc độ cao nhất
- Tự động khởi động ở Chế độ hoạt động và ẩn
- Công cụ keylogger mạnh mẽ để nắm bắt tất cả các mật khẩu
- Trình chiếu tích hợp cho ảnh chụp nhanh màn hình

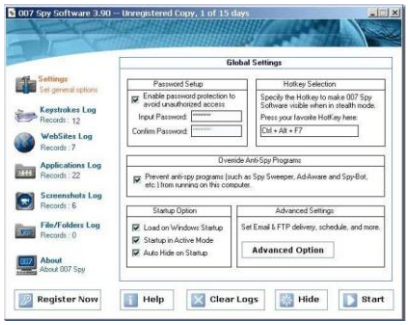
42

007 Spy Software: Screenshot 1



43

007 Spy Software: Screenshot 2



44

SpyBuddy

- SpyBuddy 2009 là một phần mềm giám sát máy tính tiết lộ những gì nhân viên đang thực sự làm việc trên máy tính
- Nó bí mật ghi lại tất cả các hoạt động liên quan đến internet và máy tính và hiện thông tin cho bạn

Tính năng:

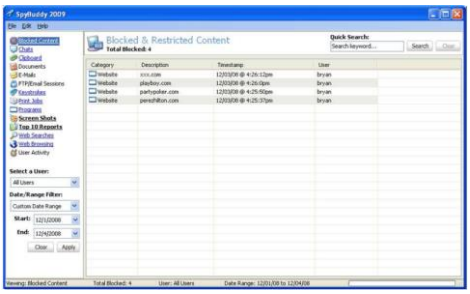
- Chặn trò chuyện
- Chặn trang web
- Giám sát hoạt động của khay nhớ tạm
- Ghi lại ảnh chụp màn hình
- Các tổ hợp phím đã nhập ghi âm
- Ghi âm tìm kiếm trực tuyến
- Giám sát hoạt động in

45

SpyBuddy 2009: Screenshot 1

46

SpyBuddy 2009: Screenshot 2



47

SoftActivity Keylogger

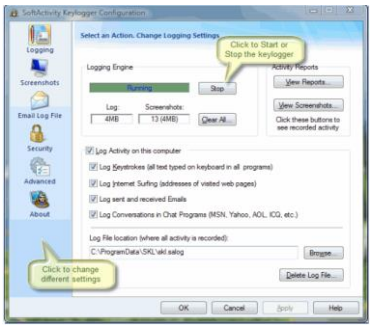
- SoftActivity Keylogger là một công cụ gián điệp chạy trong nền vàghi lại bí mật các URL đã truy cập trong trình duyệt, các lần gõ phím trong bất kỳ chương trình nào, trò chuyệncuộc trò chuyện, nhận và gửi email
- Nó chụp ảnh chụp màn hình của máy tính để bàn tại một khoảng thời gian định sẵn

Tính năng:

- Ghi lại mọi thứ
- Ghi lại ảnh chụp màn hình với công nghệ IntelliSnap™ tiên tiến
- Các tính năng báo cáo nâng cao
- Hoạt động bí mật
- Nhận báo cáo qua email

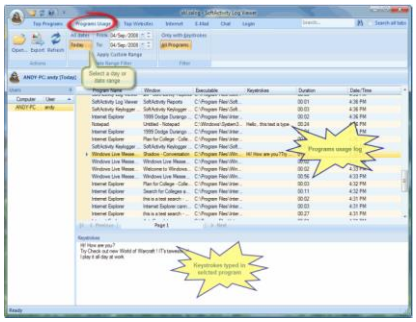
48

SoftActivity Keylogger: Screenshot 1



49

SoftActivity Keylogger: Screenshot 2



50

Elite Keylogger

Elite Keystroke là keylogger cho phép quan san và ghi lại mọi chi tiết về hoạt động trên PC và Internet

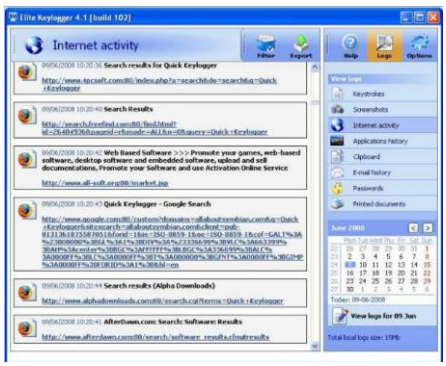
Tính năng
- Ghi lại tổ hợp phím
- Không bị phát hiện
- Ghi lại thông tin Email, tin nhắn, ...
- Giám sát khay nhớ tạm
- Ghi lại hoạt động ứng dụng
- Giám sát Winlogon và mật khẩu
- Ghi lại ảnh chụp màn hình

51

Elite Keylogger: Screenshot 1

52

Elite Keylogger: Screenshot 2



53

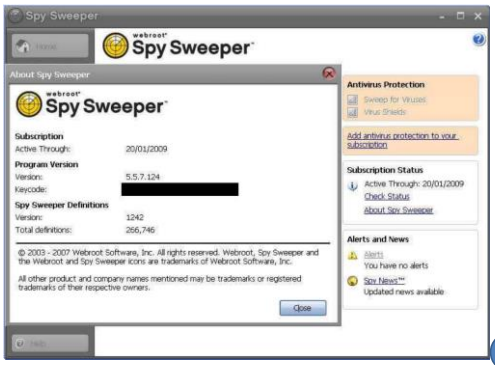
Spy Sweeper

- Spy Sweeper là phần mềm chống và xóa phần mềm gián điệp
- Nó cung cấp khả năng phát hiện phần mềm gián điệp tiên tiến có sẵn để đánh bại các chương trình phần mềm gián điệp nguy hiểm

Tính năng:
- Khả năng phát hiện và loại bỏ nâng cao
- Phát hiện nguy cơ theo thời gian
- Phương pháp phát hiện rootkit nâng cao
- Ít ảnh hưởng tới chất lượng hoạt động của hệ thống
- Phù hợp với Windows vista
- Bảo vệ được nhiều người dùng
- Cập nhật thông tin mới về phần mềm gián điệp

54

Spy Sweeper: Screenshot 1



55

Summary

- Người trong cuộc thực hiện các hoạt động độc hại trên mạng, hệ thống và cơ sở dữ liệu của tổ chức
- Phản ứng phụ thuộc vào bản chất của các mối đe dọa nội bộ và chính sách của tổ chức
- Các mối đe dọa nội bộ có thể được phát hiện bằng cách kiểm tra nhật ký sự kiện hệ thống bao gồm nhật ký cơ sở dữ liệu, nhật ký email, nhật ký ứng dụng, nhật ký truy cập tệp và nhật ký truy cập từ xa
- Các đặc quyền truy cập phải được bật cho nhân viên hoặc người dùng dựa trên hiệu suất thường xuyên của các vai trò công việc của họ
- Các tổ chức nên thực hiện các quy trình sao lưu và phục hồi an toàn để tiếp tục hoạt động kinh doanh khi hệ thống bị xâm phạm

56