**MỤC LỤC**

[CHƯƠNG 1. TỔNG QUAN VỀ PHẦN MỀM ĐỘC HẠI VÀ CÁC VẤN ĐỀ LIÊN QUAN ĐẾN AN NINH MẠNG 1](#_Toc92223120)

[1.1. Khái niệm về phần mềm độc hại 1](#_Toc92223121)

[1.2. Cái nhìn tổng quan về Malware trên thiết bị di động 1](#_Toc92223122)

[1.2.1. Malware trên thiết bị di động 1](#_Toc92223123)

[1.2.2. Những thông tin mà Malware có thể khai thác trên điện thoại 1](#_Toc92223124)

[1.2.3. Các cách phòng chống thất thoát thông tin 2](#_Toc92223125)

[CHƯƠNG 2. THỐNG KÊ VỀ PHẦM MỀM ĐỘC HẠI CỦA HÃNG BẢO MẬT KASPERSKY 3](#_Toc92223126)

[2.1. Chương trình độc hại trên Internet (các cuộc tấn công thông qua web) 3](#_Toc92223127)

[2.1.1. Top 20 chương trình độc hại trên Internet 3](#_Toc92223128)

[2.1.2. Top 15 quốc gia có các website nguy cơ lây nhiễm bới các phần mềm độc hại 3](#_Toc92223129)

[2.2. Nguồn phát tán các phần mềm độc hại 4](#_Toc92223130)

[2.3. Các ứng dụng dễ trở thành nạn nhân của phần mềm độc hại 4](#_Toc92223131)

# TỔNG QUAN VỀ PHẦN MỀM ĐỘC HẠI VÀ CÁC VẤN ĐỀ LIÊN QUAN ĐẾN AN NINH MẠNG

## Khái niệm về phần mềm độc hại

Phần mềm ác ý hay phần mềm ác tính, phần mềm độc hại (tiếng Anh: malware là sự ghép của hai chữ malicious và software) là một loại phần mềm hệ thống do các tay tin tặc hay các kẻ nghịch ngợm tạo ra nhằm gây hại cho các máy tính. Tùy theo cách thức mà tin tặc dùng, sự nguy hại của các loại phần mềm ác ý có khác nhau từ chỗ chỉ hiển thị các cửa sổ hù dọa cho đến việc tấn công chiếm máy và lây lan sang các máy khác như là virus trong cơ thể của các sinh vật.

Do định nghĩa, từ phần mềm ác ý sẽ bao gồm các lọai phần mềm sau:

* Virus : các dạng mã độc nhiễm trực tiếp vào tệp;
* Worm : sâu máy tính;
* Trojan : còn có tên gọi khác là Trojan horse – Ngựa thành Troia;
* Spyware: tự động ghi lại các thông tin của máy tính bị xâm nhập;
* Adware : tự động hiện các bản quảng cáo;
* Keyloger: ghi nhận lại toàn bộ thao tác của bàn phím;
* Backdoor: mở cửa hậu cho kẻ khác xâm nhập;
* Rootkit : phần mềm mã độc tổng hợp.

## Cái nhìn tổng quan về Malware trên thiết bị di động

### Malware trên thiết bị di động

Như chúng ta đã biết Malware (phần mềm ác tính) viết tắt của cụm từ Malicious Sofware, là một phần mềm máy tính được thiết kế với mục đích thâm nhập hoặc gây hỏng hóc máy tính mà người sử dụng không hề hay biết.

Theo thống kê của các hãng bảo mật trên thế giới thì hiện các Malware hiện nay mới chỉ dừng lại ở mức độ xâm nhập và ăn cắp thông tin của người dùng và nó chưa có cơ chế lây lan. Theo các kết quả trên thì Malware trên Smartphone hiện nay về cách thức hoạt động giống như một phần mềm gián điệp (Trojan) hơn là một virus phá hủy.

### Những thông tin mà Malware có thể khai thác trên điện thoại

DroidDream được coi là một trong những Malware đầu tiên trên Android, mục đích của con DroidDream này mới chỉ dừng lại ở mức độ làm cho chiếc điện thoại của bạn tự động cài đặt những ứng dụng chứa mã độc khác. Tuy nhiên các biến thể của nó đã kịp thời biến đổi để gây ra các mối nguy hại lớn hơn rất nhiều. Như con « Hippo SMS« được tìm thấy mới đây có khả năng tự gửi tin nhắn mà không cần sự cho phép của người dùng, việc này sẽ khiến tiền cước phí của bạn tăng lên một cách chóng mặt mà bạn không biết rõ lí do tại sao.

### Các cách phòng chống thất thoát thông tin

Khi sử dụng các thiết bị di động, người dùng cần chú ý tới các vấn đề sau:

* Luôn luôn tìm hiểu kỹ thông tin từ:
* Nhà cung cấp các phần mềm;
* Tác giả của các ứng dụng.
* Đọc các bài viết trên mạng, các lời bình luận liên quan tới ứng dụng đó;
* Luôn luôn đọc thật kỹ các quyền hạn của ứng dụng đó;
* Cài đặt một ứng dụng Anti Virus để tiêu diệt và phát hiệt các Malware.

# THỐNG KÊ VỀ PHẦM MỀM ĐỘC HẠI CỦA HÃNG BẢO MẬT KASPERSKY

## Chương trình độc hại trên Internet (các cuộc tấn công thông qua web)

Số lượng các cuộc tấn công dựa trên trình duyệt năm 2011 tăng từ 580.371.937 đến 946.393.693. Điều đó có nghĩa là các sản phẩm của Kaspersky Lab bảo vệ người dùng khi họ lướt Internet ở mức trung bình 2.592.859 lần mỗi ngày.

Số lượng các cuộc tấn công dựa trên web trong năm 2011 là 1,63 lần so với tổng cho năm 2010, mà điểm đến một tỷ lệ tăng trưởng chậm hơn nhiều hơn so với chúng ta đã thấy trong quá trình ba năm qua. Trong năm 2010, chúng tôi ghi nhận một sự đột biến các phần mềm mã độc, lớn hơn rất nhiều so với năm trước (gấp 8 lần so với năm 2009).

Tốc độ tăng trưởng chậm lại nỗ lực lây nhiễm dựa trên web là do thực tế là vào năm 2011 người sử dụng độc hại đã không sử dụng bất kỳ phương pháp cơ bản mới nhiễm hàng loạt tung ra các cuộc tấn công chống lại các máy tính. Vũ khí chính của nhiễm trùng dựa trên trình duyệt vẫn còn các gói khai thác, cho phép người sử dụng độc hại để khởi động ổ đĩa bởi các cuộc tấn công mà không có nạn nhân nhận thấy một điều. Trong suốt năm nay, hai bộ sưu tập khai thác đã được bán trên thị trường chợ đen: Blackhole, và Incognito, đó là một hit ngay lập tức giữa các bọn tội phạm mạng và trở thành hai trong số đầu năm phổ biến nhất được sử dụng khai thác gói. Ngẫu nhiên, doanh nghiệp này hầu như hoàn toàn được xây dựng theo chương trình liên kết được thiết lập bởi tin tặc.

### Top 20 chương trình độc hại trên Internet

Những số liệu thống kê thể hiện bản án là phát hiện của các mô-đun chống virus dựa trên web và đã được đệ trình bởi người sử dụng của sản phẩm Kaspersky Lab đã đồng ý chia sẻ dữ liệu địa phương của họ.

Sự phát triển của công nghệ phát hiện mới cho KSN đã giúp tăng tỷ lệ phần trăm của các mối đe dọa được phát hiện thông qua các phương pháp phỏng đoán và không có cập nhật cơ sở dữ liệu chống virus truyền thống - từ 60% đến 75%. Các trang web độc hại phát hiện bằng cách sử dụng những phương pháp này đã được xếp hạng ở vị trí đầu tiên. Lưu ý rằng hầu hết các phát hiện URL độc hại cho các trang web với khai thác.

Danh sách dưới đây cho thấy các chương trình độc hại được sử dụng phổ biến nhất liên quan đến các cuộc tấn công Internet với các đối tượng sử dụng.

### Top 15 quốc gia có các website nguy cơ lây nhiễm bới các phần mềm độc hại

Trong 946.393.693 cuộc tấn công web, tội phạm mạng đã sử dụng 4.073.646 tên miền. Máy chủ hạt giống với mã độc hại đã được phát hiện trong các khu vực Internet của 198 quốc gia trên khắp thế giới, dưới đây là top 15 quốc gia có các website nguy cơ bị lây nhiễm bởi các phần mềm độc hại, chiếm 86,4% của tất cả các lưu trữ độc hại được phát hiện bởi Kaspersky Lab.

## Nguồn phát tán các phần mềm độc hại

Báo cáo phân loại các trang web thường xuyên cố gắng để thu hút người sử dụng KSN thông qua các liên kết độc hại, và trong năm 2011, có 20 website thường xuyên nhất chuyển hướng tới các phần mềm độc hại thuộc các nhóm sau đây:

## Các ứng dụng dễ trở thành nạn nhân của phần mềm độc hại

Một phân tích về khai thác được sử dụng phổ biến nhất đã giúp xác định các chương trình thường xuyên nhất nhìn thấy chỗ yếu của họ nhắm mục tiêu của tin tặc trong năm 2011.