

BITDEFENDER VỀ XU THẾ PHÁT TRIỂN VƯỢT TRỘI CỦA TROJANS VÀ CÁC NGUY CƠ TRONG NĂM 2009

Hơn 80% mã độc được phát triển trên thế giới là Trojans, theo đánh giá của E-Threats Landscape Report, một tài liệu nghiên cứu toàn diện về các mối đe dọa được xuất bản bởi BitDefender®, nhà cung cấp hàng đầu về những giải pháp bảo mật dữ liệu và phần mềm chống virus. Báo cáo tổng kết này, lần thứ hai trong loạt các báo cáo bảo mật, cung cấp một cái nhìn toàn diện về những mối đe dọa bảo mật trong năm 2008 và những dự đoán cho năm 2009.

Các chuyên gia bảo mật của BitDefender nhận thấy rằng, người sử dụng Internet mỗi ngày phải đối phó với xấp xỉ 2000 virus mới (bao gồm cả biến thể), gần 50.000 vụ lừa đảo trực tuyến mỗi tháng và hơn 1.000.000 máy tính bị lợi dụng làm bots để phát tán rootkits, Trojans và các mã độc khác trong năm.

Những điều cần lưu ý từ báo cáo của BitDefender bao gồm:

- Mức độ tăng của các hiểm họa từ Internet là trên 460%;
- Sự khai thác lỗi JavaScript truy vấn SQL tăng gấp ba lần;
- 75% Trojans tích hợp nhiều cơ chế thông minh như: cơ chế tự cập nhật và đặc tính nạp dữ liệu, cơ chế tải tệp xuống tự động và lén lút tăng khả năng gián điệp và chiếm quyền;
- Những hàng tit chung nhất thường dùng để lan truyền mã độc bao gồm các thông tin về những người nổi tiếng và đặc biệt là những sự kiện nổi bật, giật gân;
- Thư điện tử với văn bản thuần có tới 80% là spam, trong thư có ảnh thì spam lại giảm còn 1.5%;
- Số lượng thư điện tử spam chứa đựng những mã độc đính kèm hay các liên kết chứa mã độc tăng 400%;

- Những nước phát tán mã độc nhiều nhất là Pháp, Trung Quốc, Hoa Kỳ, Đức và Tây Ban Nha;
- Gần 70% các vụ lừa đảo trực tuyến nhắm vào ngành tài chính trên toàn cầu;
- Kỹ thuật spam mới mimicking- bắt trước, làm theo, và thông báo mới từ những tập đoàn thông tin như CNN, CBS và ABC đã được giới thiệu;
- Người tạo ra spam tập trung sự chú ý của họ vào những thông báo biên lai để tăng hiệu quả.

Báo cáo dự đoán các hiểm họa trong năm 2009 bao gồm:

- Nền công nghệ sản xuất mã độc sẽ tiếp tục lợi dụng những khả năng trên nền mạng của Trojans và rootkit để làm gián điệp ăn cắp thông tin;
- Gia đình mã độc cũng sẽ được nâng cấp và có những thay đổi quan trọng tăng cường khả năng hành động lén lút và tự động hóa;
- Một sự tăng trưởng khác sẽ nhắm vào khai thác những điểm yếu trong ứng dụng, mà chủ yếu là ăn cắp mật khẩu (Trojans.PWS.ChromeInject.A là điển hình). Các chuyên gia của BitDefender cũng xác định vào khoảng trước tháng mười hai, khả năng tấn công nhắm tới các ứng dụng trên nền Web 2.0 sẽ tăng;
- Những thiết bị di động thông minh như SmatrPhone,... với khả năng tự truy nhập thường xuyên cũng sẽ là mục tiêu nhắm tới của các malware di động.

Lê Ngọc Quang