CÁC XU HƯỚNG TẤN CÔNG TRÊN MẠNG NĂM 2016 VÀ CÁC GIẢI PHÁP PHÒNG CHỐNG

Nguyễn Ngọc Cương,

Cục CNTT

Hà Nội, 03. 2016

AGENDA

- Tóm tắt
- Các xu hướng tấn công trên mạng năm 2016
- Các giải pháp phòng chống?

TÓM TẮT

- Sự phát triển vũ bão của mạng thông tin di động với đa dạng loại hình dịch vụ trực tuyến, cùng với sự bùng nổ trào lưu xây dựng phát triển và cung cấp ứng dụng, dịch vụ trên điện toán đám mây cũng như các ứng dụng mạng xã hội dẫn đến thách thức to lớn cho việc phòng chống và bảo vệ an ninh an toàn thông tin trong xã hội công nghệ hiện tại.
- Các hình thức tấn công mạng, tấn công dữ liệu và các loại hình tội phạm mạng ngày càng tinh vi đòi hỏi các giải pháp, các đơn vị chuyên trách phải luôn đầu tư chuyên sâu để nâng cấp phòng chống và phát hiện các nguy cơ tấn công

CÁC XU HƯỚNG TẤN CÔNG TRÊN MẠNG NĂM 2016

- Tấn công trên diện rộng của mã độc mã hóa dữ liệu để tống tiền (Ransomware):
  - Xuất hiện từ những năm 2005-2006 và trở nên đặc biệt nguy hiểm với biến thể virus CryptoLocker vào cuối 2013.
  - Thực sự tồi tệ hơn theo hàng năm khi các tin tặc có thể nhận miễn phí mã nguồn để thay đổi theo các mục đích riêng
  - Loại tấn công này sẽ mã hóa các tập tin quan trọng, làm cho dữ liệu không truy cập được cho đến khi trả tiền chuộc.
  - Không chỉ tấn công các máy tính cá nhân mà còn khóa các tập tin trên mạng, có thể xuất hiện trên điện thoại thông minh hay máy tính bảng.

CÁC XU HƯỚNG TẤN CÔNG TRÊN MẠNG NĂM 2016

- Hardware:
  - Tấn công dựa trên phần cứng không phải là thuật ngữ mới, tuy nhiên gần đây được phát hiện khá nhiều và được dự đoán phát triển mạnh trong năm 2016
  - Một số hình thức:
    - USB flash: Equation Group vừa phát hiện chương trình mã độc cài trong các USB flash để tiến hành giám sát mục tiêu. Các sâu này không thể loại bỏ kể cả khi định dạng lại ổ đĩa
    - Cài sẵn mã độc trong BIOS của máy tính, cài sẵn mã theo dõi trong các chương trình tiện tích riêng của hãng máy tính
    - Cài sẵn mã trong các firrmware của thiết bị
    - Tích hợp mã độc trên IC (Trojan circuit / Hardware Trojan)

CÁC XU HƯỚNG TẤN CÔNG TRÊN MẠNG NĂM 2016

- Spear-phishing:
  - Xu hướng tấn công thư giả mạo đã xuất hiện từ lâu nhưng vẫn tiếp tục là một xu hướng diễn biến phức tạp và tăng cao nguy cơ đe dọa người dùng trong năm 2016.
  - Xu hướng này ngày càng được nâng cấp khi được gửi từ các địa chỉ đã biết rõ khiến những thư gian lận này rất khó để phát hiện
  - Nhân lực thực thi phát tán thư lừa đảo được đào tạo theo từng chiến dịch phát tán

CÁC XU HƯỚNG TẤN CÔNG TRÊN MẠNG NĂM 2016

- Browser Plug-in:
  - Hãng Ofcom (Anh) gần đây phát hiện rằng người lớn thường dành trung bình 20 giờ mỗi tuần để sự dụng dịch vụ trực tuyến, mà chủ yếu là dành cho trình duyệt web → nguồn tập trung tấn công của tin tặc
  - Năm 2015 đã ghi nhận nhiều trường hợp tin tặc tấn công vào các yếu điểm của trình duyệt web, đặc biệt nhắm vào adobe flash để thực thi các quảng cáo độc hại
  - Xu hướng này được đánh giá sẽ bùng nổ trong năm 2016

CÁC XU HƯỚNG TẤN CÔNG TRÊN MẠNG NĂM 2016

- Dịch vụ điện toán đám mây (Cloud services):
  - Dịch vụ điện toán đám mây bùng nổ kèm theo xu hướng gia tăng các xu hướng tấn công trên đám mây
  - Cloud malware: một loại hình cài mã độc mới được đánh giá sẽ chuyển hướng tấn công sang điện toán đám mây trong năm 2016, gây ảnh hưởng lớn đến khả năng tính toán, cơ sở hạ tầng, các ứng dụng và dữ liệu.
  - Tính bảo mật, nguyên vẹn dữ liệu trên luôn là vấn đề trở ngại cho việc khai thác trên điện toán đám mây

CÁC XU HƯỚNG TẤN CÔNG TRÊN MẠNG NĂM 2016

- Các xu hướng phổ biến khác như tấn công bằng phần mềm gián điệp (spyware), tấn công từ chối dịch vụ (DDOS), tấn công bằng mã độc trên mạng xã hội vẫn tiếp tục gia tăng trong năm 2016 và ngày càng mang nhiều yếu tố chính trị.

GIẢI PHÁP PHÒNG CHỐNG?

- Trên thực tế, chưa có một giải pháp toàn diện cho việc phòng chống các loại hình tấn công trên mạng.
- Phòng chống các nguy cơ tấn công mạng không phải trách nhiệm của một cá nhân hay tổ chức, mà là của cộng đồng.

GIẢI PHÁP PHÒNG CHỐNG?

- Đào tạo nâng cao nhận thức và kỹ năng khai thác dịch vụ cho người sử dụng.
- Phát triển và tối ưu nguồn lực, vật lực và nhân lực chuyên trách an ninh mạng.
- Thay đổi quan điểm phòng chống tấn công: phòng chống không chỉ từ bên ngoài mà ngay cả từ bên trong nội bộ.
- Triển khai các hệ thống giám sát bảo vệ toàn mạng nhằm tự động phát hiện và cô lập các truy cập/hoạt động trái phép trên mạng nội bộ và mạng diện rộng dùng riêng (nghe lén, phát tán mã độc, …).
- Xây dựng chính sách phòng chống APT (Advanced persistent threat) ngay từ bên trong mạng nội bộ.

Thank You!