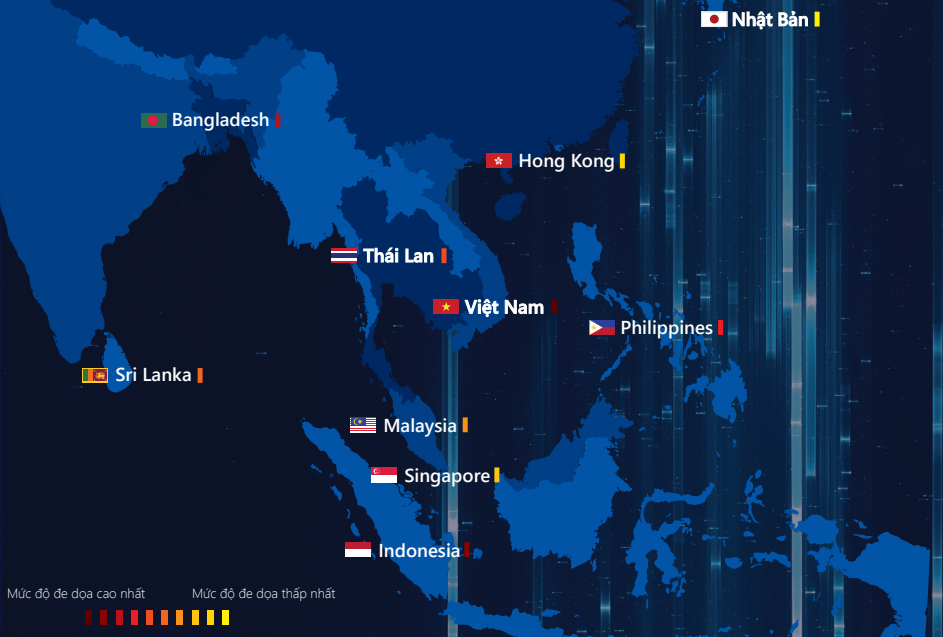
Toàn cảnh mối đe dọa từ mã độc ở khu vực Châu Á Thái Bình Dương 2017

Microsoft

Với sự gia tăng của các trường hợp lây nhiễm mã độc và các mối đe dọa mạng tinh vi, an ninh đang trở thành ưu tiên hàng đầu đối với hầu hết các tổ chức. Microsoft đầu tư hơn 1 tỷ USD hàng năm vào nghiên cứu và phát triển trong lĩnh vực an ninh, bao gồm cả việc điều tra các dòng mã độc mới xuất hiện. Dưới đây là toàn cảnh mối đe dọa này:

TOP THỊ TRƯỜNG BỊ ĐE DỌA BỞI MÃ ĐỘC Ở KHU VỰC CHÂU Á THÁI BÌNH DƯƠNG



TOP MÃ ĐỘC PHỔ BIẾN Ở KHU VỰC CHÂU Á THÁI BÌNH DƯƠNG

1. **Gamarue**: Cho phép tin tặc kiểm soát máy tính của bạn, đánh cắp thông tin và thay đổi thiết lập bảo mật của máy tính.
2. **Lodbak**: Thường được cài đặt bởi Gamarue trên các ổ đĩa di động, và sẽ cố cài đặt Gamarue khi ổ đĩa bị nhiễm độc được kết nối với máy tính khác.
3. **Dynamer**: Đánh cắp thông tin cá nhân, tải về thêm nhiều mã độc hoặc cho phép tin tặc truy cập vào máy tính.
4. **Axpergle**: Lợi dụng lỗ hổng phần mềm để cài đặt mã độc trên máy tính.
5. **Spursint**: Nhân cơ hội người dùng mắc sai lầm hoặc truy cập website độc hại để xâm nhập vào máy tính. Đánh cắp dữ liệu của người dùng hoặc cho phép tin tặc truy cập từ xa.

MẸO BẢO ĐẢM AN NINH MẠNG cho **CÁ NHÂN**

NGUYÊN TẮC CƠ BẢN
Chỉ sử dụng phần mềm chính hãng và đang lưu hành, có nguồn gốc đáng tin cậy; luôn cập nhật hệ điều hành và sử dụng các chương trình chống virus mạnh mẽ.

QUẢN LÝ MẬT KHẨU
Sử dụng mật khẩu mạnh cho mỗi tài khoản và thay đổi mật khẩu thường xuyên.

KHÔI PHỤC
Sao lưu dữ liệu của bạn một cách định kỳ trên các dịch vụ lưu trữ đám mây đáng tin cậy.

LUÔN CẢNH GIÁC
Các hoạt động nhạy cảm như dịch vụ ngân hàng trực tuyến và các giao dịch qua mạng Internet chỉ nên được thực hiện trên thiết bị cá nhân của bạn và trên một mạng tin cậy.

GIÁM SÁT
Theo dõi và cảnh giác trước bất kỳ hoạt động lạ hoặc đáng ngờ nào trên tất cả các tài khoản trực tuyến của bạn vì đây có thể là dấu hiệu của hành vi xâm nhập.

MẸO BẢO ĐẢM AN NINH MẠNG cho **TỔ CHỨC**

LÀM SẠCH KHÔNG GIAN MẠNG
Duy trì các hoạt động Internet an toàn hơn tại nơi làm việc và các chính sách CNTT nội bộ mạnh mẽ.

QUẢN LÝ CNTT
Hoạt động quản lý tài sản phần mềm mạnh mẽ (ISO/IEC 19770); Ưu tiên vá lỗi bảo mật; Sử dụng phần mềm cập nhật.

VĂN HOÁ DỮ LIỆU
Phân loại dữ liệu và kiểm soát truy cập; phân tích dữ liệu lớn để phát hiện các hành vi sai trái, các cuộc tấn công và các vi phạm tiềm tàng.

HỆ THỐNG PHÒNG THỦ MẠNG
Sử dụng hệ điều hành có các giải pháp chống mã độc được tích hợp sẵn và đáng tin cậy. Sử dụng biện pháp xác thực đa yếu tố (MFA) và mã hóa thiết bị.

KIỂM TOÁN AN NINH
Định kỳ đánh giá việc giám sát mối đe dọa, các giao thức an ninh và chuỗi cung ứng CNTT.

MICROSOFT CÓ THỂ GIÚP BẠN CỦNG CỐ AN NINH BẢO MẬT NHƯ THẾ NÀO

BẢO VỆ: Cung cấp sự bảo vệ cho tất cả các thiết bị đầu cuối từ các cảm biến đến trung tâm dữ liệu để ngăn chặn các cuộc tấn công mạng.

PHÁT HIỆN: Giám sát và phát hiện các lỗ hổng tấn công và các mối đe dọa dai dẳng bằng cách sử dụng các tín hiệu mục tiêu, giám sát hành vi và phương pháp phân tích dữ liệu Machine learning.

ỨNG PHÓ: Điều tra và làm gián đoạn các sự kiện đáng ngờ để cung cấp sự chẩn đoán và đề xuất các biện pháp giải quyết, thu hẹp khoảng cách giữa phát hiện và hành động.

Để tìm hiểu thêm về biện pháp chống lại các cuộc tấn công mạng của Microsoft, vui lòng truy cập **www.microsoft.com/security**