Tiêu đề: Doanh nghiệp Việt không biết chống mã độc tống tiền từ đâu
Tác giả: Thanh Trực - Đức Thiện
Nguồn: Tuổi Trẻ đăng ngày 18/05/2017
Đường dẫn bài viết: http://nhipsongso.tuoitre.vn/tin/20170518/doanh-nghiep-viet-khong-biet-chong-ma-doc-tong-tien-tu-dau/1316778.html

Doanh nghiệp Việt không biết chống mã độc tống tiền từ đâu

18/05/2017 17:00 GMT+7

TTO - Cuộc tấn công của mã độc WannaCry một lần nữa cho thấy sự bị động của nhiều doanh nghiệp, tổ chức tại Việt Nam, loay hoay tìm cách ứng phó, không biết bắt đầu từ đâu?

WannaCry thật sự là cơn ác mộng cho các hệ thống máy tính doanh nghiệp, và cơn ác mộng này chưa dừng lại - Ảnh minh họa: NewsBTC

Theo công bố của Trung tâm ứng cứu khẩn cấp máy tính Việt Nam (VNCERT), đến ngày 18-5, lượng máy tính bị nhiễm mã độc WannaCry trong nước đã giảm nhiều, chỉ còn vài trường hợp.

Tuy nhiên theo công bố của Công ty an ninh mạng Bkav, với 52% máy tính tại Việt Nam - tương đương khoảng 4 triệu máy - chưa được vá lỗ hổng EternalBlue, khiến các máy này có thể bị nhiễm WannaCry bất cứ lúc nào nếu hacker mở rộng cuộc tấn công.

Thiếu kịch bản phòng thủ

Ấn phẩm này chỉ nhằm mục đích cung cấp hướng dẫn tổng quát và không nên sử dụng để đưa ra quyết định cụ thể.
Để biết thêm thông tin, vui lòng liên hệ:
Chị Vũ Thị Thu Nguyệt, Trưởng phòng Truyền thông và Marketing, ĐT: +84 4 3946 2246, máy lẻ 4690, Email: vu.thi.thu.nguyet@vn.pwc.com

Tiêu đề: Doanh nghiệp Việt không biết chống mã độc tống tiền từ đâu
Tác giả: Thanh Trực - Đức Thiện
Nguồn: Tuổi Trẻ đăng ngày 18/05/2017
Đường dẫn bài viết: http://nhipsongso.tuoitre.vn/tin/20170518/doanh-nghiep-viet-khong-biet-chong-ma-doc-tong-tien-tu-dau/1316778.html

Các chuyên gia an ninh mạng và các công ty bảo mật vừa qua liên tục nhận được nhiều yêu cầu trợ giúp giải quyết tình trạng nhiễm độc hoặc tư vấn giải pháp bảo vệ hệ thống máy tính... Nhận xét của các chuyên gia an ninh mạng là hầu hết các doanh nghiệp đều hết sức bị động trước chiến dịch tấn công mạng.

> **Việt Nam trong tốp 20 quốc gia bị lây nhiễm nhiều nhất dù Việt Nam không phải là tâm điểm hacker nhắm đến trong cuộc tấn công này**
>
> *Hãng bảo mật Kaspersky Lab*

Trao đổi với Tuổi Trẻ về nguyên do vì sao Việt Nam nằm trong nhóm các quốc gia có tỉ lệ lây nhiễm và ảnh hưởng bởi WannaCry, ông Robert Trọng Trần – Giám đốc Dịch vụ An ninh mạng, Công ty PwC Việt Nam cho rằng do các doanh nghiệp, tổ chức tại Việt Nam vẫn đang sử dụng các thiết bị và phần mềm cũ, cản trở việc cài đặt và chạy các bản vá lỗi (patch) một cách dễ dàng.

* Kiến thức bảo mật của người Việt Nam: Lỗ hổng để tấn công mạng

Theo ông Robert Trọng Trần, lẽ ra nhiều tổ chức và doanh nghiệp đã có thể tránh được cuộc tấn công bởi mã độc tống tiền này vì từ ngày 14-3 năm nay, Microsoft đã đưa ra bản vá cho lỗi này. Vì vậy, những máy tính chưa cập nhật bản vá Windows MS17-010 đều có thể là mục tiêu tấn công của WannaCry.

Bên cạnh đó, ông Robert cho biết một yếu tố rất quan trọng mà các doanh nghiệp đã bỏ qua khiến đơn vị của mình bị ảnh hưởng nặng nề hơn khi đối mặt tấn công mạng, đó là kịch bản phản ứng nhanh sự cố mạng.

"Nếu các doanh nghiệp đã chuẩn bị sẵn một kịch bản phản ứng nhanh, hay còn gọi là "playbook" để ứng phó với các sự cố an ninh mạng thì họ đã có thể giảm thiểu sự lan rộng của WannaCry. Nếu có một kịch bản phản ứng nhanh, có khả năng vận hành và điều phối tự động (automation and orchestration) thì các doanh nghiệp có thể phát hiện và kiểm soát các mã độc tống tiền trước khi nó phát tán ra toàn mạng lưới nội bộ."

Trong khi đó, theo Bkav, việc phát tán mã độc mã hóa tống tiền WannaCry chỉ là bề nổi của "tảng băng chìm".

Ông Vũ Ngọc Sơn, Phó chủ tịch phụ trách mảng chống mã độc (Anti Malware) của Bkav phân tích: "Chúng ta không nên quên Cơ quan an ninh Mỹ NSA được cho là đã sử dụng lỗ hổng này để do thám. Do đó, không loại trừ khả năng cơ quan gián điệp của một quốc gia khác cũng âm thầm khai thác lỗ hổng này, cài đặt phần mềm gián điệp nằm vùng để thực hiện các cuộc tấn công có chủ đích APT".

Suy nghĩ chủ quan: họ không nhắm đến mình đâu!

Chia sẻ với Tuổi Trẻ, ông Robert Trọng Trần nói: "Một sai lầm về nhận thức mà nhiều doanh nghiệp vừa và nhỏ đang mắc phải, đó là cho rằng mình quá nhỏ bé để trở thành mục tiêu của tin tặc. Điều này hoàn toàn không đúng. Họ chính là những mục tiêu dễ dàng và phổ biến nhất của các tội phạm mạng.

Ấn phẩm này chỉ nhằm mục đích cung cấp hướng dẫn tổng quát và không nên sử dụng để đưa ra quyết định cụ thể.
Để biết thêm thông tin, vui lòng liên hệ:
Chị Vũ Thị Thu Nguyệt, Trưởng phòng Truyền thông và Marketing, ĐT: +84 4 3946 2246, máy lẻ 4690, Email: vu.thi.thu.nguyet@vn.pwc.com

Tiêu đề: Doanh nghiệp Việt không biết chống mã độc tống tiền từ đâu
Tác giả: Thanh Trực - Đức Thiện
Nguồn: Tuổi Trẻ đăng ngày 18/05/2017
Đường dẫn bài viết: http://nhipsongso.tuoitre.vn/tin/20170518/doanh-nghiep-viet-khong-biet-chong-ma-doc-tong-tien-tu-dau/1316778.html

Ông Robert Trọng Trần, Giám đốc Dịch vụ An ninh mạng, Công ty PwC Việt Nam

* Xem: Doanh nghiệp cần chú trọng an toàn thông tin hơn

Rất nhiều doanh nghiệp vừa và nhỏ trở thành nạn nhân của các cuộc tấn công mạng vì họ thường không có bộ phận công nghệ thông tin chuyên trách hoặc không có chuyên gia về an ninh mạng trong bộ phận đó. Thực tế là rất nhiều doanh nghiệp vừa và nhỏ Việt Nam đã bị tấn công và phần lớn trong số họ chọn phương án là trả tiền cho tội phạm mạng."

> **Các doanh nghiệp và tổ chức không thể tránh khỏi mối đe dọa từ các vụ tấn công an ninh mạng. Họ phải chuẩn bị đầy đủ về mặt con người, quy trình và công nghệ để ứng phó khi bị tấn công**
>
> *Ông Robert Trọng Trần*

Đáng chú ý, giới chuyên gia an ninh mạng trên thế giới đang liên tục cảnh báo về sự xuất hiện các biến thể mới khó ngăn chặn hơn của mã độc tống tiền WannaCry đồng thời nhận thấy những cuộc tấn công mới đã bắt đầu.

Ấn phẩm này chỉ nhằm mục đích cung cấp hướng dẫn tổng quát và không nên sử dụng để đưa ra quyết định cụ thể.
Để biết thêm thông tin, vui lòng liên hệ:
Chị Vũ Thị Thu Nguyệt, Trưởng phòng Truyền thông và Marketing, ĐT: +84 4 3946 2246, máy lẻ 4690, Email: vu.thi.thu.nguyet@vn.pwc.com

Tiêu đề: Doanh nghiệp Việt không biết chống mã độc tống tiền từ đâu
Tác giả: Thanh Trực - Đức Thiện
Nguồn: Tuổi Trẻ đăng ngày 18/05/2017
Đường dẫn bài viết: http://nhipsongso.tuoitre.vn/tin/20170518/doanh-nghiep-viet-khong-biet-chong-ma-doc-tong-tien-tu-dau/1316778.html

Ông Robert Trọng Trần giới thiệu một số những nguyên tắc cơ bản sau:

- Việc bị tấn công không phải là vấn đề "có hay không" mà là "khi nào".

- Cần chuyển từ tâm lý "phòng ngừa" sang "phát hiện": mục tiêu chính là phải phát hiện được các vụ tấn công sớm nhất có thể, trước khi kẻ xấu có thể đánh cắp những dữ liệu quan trọng từ hệ thống

- Những gì có thể xảy ra sẽ xảy ra: nếu vụ tấn công dẫn tới việc đánh cắp các dữ liệu quan trọng, thì từ các đội ngũ kỹ thuật đến đội ngũ pháp lý và ban lãnh đạo, v.v. sẽ phải chuẩn bị sẵn sàng để đối phó với tình huống xấu nhất.

Vì vậy, các doanh nghiệp, tổ chức nên phát triển các kịch bản phản ứng nhanh cho từng loại sự cố an ninh mạng như mã độc tống tiền, tấn công-từ chối-dịch vụ hệ thống mạng (DDoS), chiếm quyền điều khiển website... Một nhiệm vụ quan trọng không kém là tự động hóa các kịch bản phản ứng nhanh này và thường xuyên luyện tập theo các kịch bản đó".

QUAN TÂM 0

THANH TRỰC - ĐỨC THIỆN

Ấn phẩm này chỉ nhằm mục đích cung cấp hướng dẫn tổng quát và không nên sử dụng để đưa ra quyết định cụ thể.
Để biết thêm thông tin, vui lòng liên hệ:
Chị Vũ Thị Thu Nguyệt, Trưởng phòng Truyền thông và Marketing, ĐT: +84 4 3946 2246, máy lẻ 4690, Email: vu.thi.thu.nguyet@vn.pwc.com