BỘ CÔNG AN
CÔNG AN TỈNH THỪA THIÊN HUẾ

Số: 3191 /TB-CAT-PA81

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập – Tự do – Hạnh phúc

Thừa Thiên Huế, ngày 11 tháng 7 năm 2017

THÔNG BÁO

V/v hoạt động của biến thể mã độc tống tiền "Petya"

Qua thông báo của Bộ Công an, từ tối ngày 27/6/2017, có hàng nghìn cuộc tấn công mạng bằng biến thể của mã độc tống tiền "Petya" trên thế giới, lây nhiễm trên 2000 mục tiêu là các mạng máy tính nội bộ của nhiều quốc gia, nhất là ở Nga, Ukraina, Ba Lan, Đức. Cụ thể như sau:

1. Mã độc "**Petya**" là một dạng mã độc tống tiền (*ransomware*) rất nguy hiểm, khai thác các lỗ hổng bảo mật "**Eternal Blue**" của giao thức SMBv1 (giao thức chia sẽ tập tin của hệ điều hành Windows) tương tự như mã độc Wannacry (*Công an tỉnh đã có thông báo 2342/TB-CAT-PA81 ngày 24/5/2017 gửi các ban ngành, công an các địa phương về hoạt động của mã độc này*), đồng thời kết hợp sử dụng kỹ thuật tấn công tinh vi khác để tán phát mã độc trong mạng nội bộ.

Mã độc "Petya" có khả năng lây nhiễm trên các máy tính sử dụng hệ điều hành Microsoft Window 10, Windows Server 2008 trở về trước chưa được cập nhật bản vá MS17-010. Sau khi đã thâm nhập thành công một máy tính, "Petya" sẽ khai thác lỗ hổng bảo mật "Eternal Blue" để lây nhiễm mã độc vào các máy tính nội bộ trong mạng chưa được vá lỗ hổng này. Đối với máy tính trong mạng đã cài bản vá lỗ hổng bảo mật "Eternal Blue", "Petya" sử dụng công cụ nổi tiếng khác có tên "Mimikatz" để trích xuất thông tin tài khoản đăng nhập mạng trong bộ nhớ RAM của máy tính bị lây nhiễm (tiến trình lsass.exe), chuyển các thông tin này đến công cụ PSEXEC hoặc WMIC (công cụ của Microsoft để quản trị từ xa máy tính trong mạng qua giao diện dòng lệnh) để tiếp tục cài đặt mã độc từ xa lên các máy tính khác trong cùng mạng nội bộ. Đáng chú ý, đối với mạng máy tính sử dụng mô hình quản lý tập trung (Domain), sau khi lây nhiễm thành công một máy tính trong mạng, "Petya" có thể tấn công sang các máy chủ quản trị (Domain Controller) chưa được cập nhật bản vá MS17-010, từ đó cài đặt mã độc xuống toàn bộ các máy tính trong mạng. Ngoài ra, sau khi lây nhiễm vào máy tính mạng nội bộ, nếu phát hiện máy tính này kết nối ra mạng ngoài khác (như đồng thời kết nối ra Internet hoặc mạng WAN khác qua cơ chế NAT), "Petya" sẽ thu thập các thông số hệ thống mạng, tiếp tục tấn công sang các máy tính mạng ngoài đó nếu chúng cũng tồn tại lỗ hổng "Eternal Blue". Đây là những đặc tính rất nguy hiểm, khác cơ chế hoạt động của mã độc "Wannacry", làm bùng phát "Petya" trên diện rộng, nhất là đối với các mạng nội bộ.

Sau khi lây nhiễm vào máy tính, "Petya" chờ khoảng 10 đến 60 phút sau thời điểm lây nhiễm để ra lệnh khởi động lại máy tính (bằng cách tạo một Schedule Task trong hệ điều hành). Trong quá trình máy tính khởi động lại, mã độc không mã hóa từng tập tin mà mã hóa toàn bộ ổ cứng (trừ thư mục C:\Windows) bằng cách mã hóa bảng quản lý tệp tin MFT trong phân vùng NTFS, ghi đè phân vùng MBR (Master Boot Record) bằng một trình khởi động (loader) tùy biến kèm theo thông tin cảnh báo người dùng. Đối với mỗi máy tính nạn nhân, mã độc sinh ngẫu nhiên một khóa AES-128 để mã hóa, khóa này được tiếp tục mã hóa bằng khóa công khai RSA-2048 của tin tặc, sau đó lưu trong tệp tin README. Mã độc hiện thị thông báo yêu cầu nạn nhân trả 300 USD tiền Bitcoin để trao đổi khóa giải mã. Tính đến thời điểm 16 giờ ngay 28/6, tài khoản bitcoin của tin tặc đã nhận được 3.64 bitcoin (tương đương 9000 USD). Không giống như Wannacry, mã độc Patya yêu cầu nạn nhân gửi thông tin tài khoản tới địa chỉ email Wowsmith12345@posteo.net để xác thực thanh toán và nhận lại khóa giải mã. Hiện nay, địa chỉ email này đã bị nhà cung cấp dịch vụ thư điện tử khóa, các máy chủ điều khiển bị phát hiện cũng đã được ngăn chặn, do vậy trường hợp người dùng trả tiền cũng không nhận được khóa giải mã.

Tính đến nay, mã độc "Petya" đã lây nhiễm trên 2000 mục tiêu hệ thống mạng ở nhiều quốc gia trên thế giới như Ukraina, Nga, Ba Lan,Ý, Đức, Anh, Đan Mạch, nhưng chủ yếu tập trung vào Ukraina (60%), Nga (30%), Ba Lan (6%), Italy (2%), Đức (1%). Hãng bảo mật Kaspersky cũng đã ghi nhận những cuộc tấn công nhỏ lẻ tại các quốc gia như Mỹ, Na uy... **Tại Ukraina**, các công ty điện quốc gia và các sân bay ở thủ đô Kiev đã hứng chịu các cuộc tấn công mã độc "Petya" rất lớn, được cho "chưa từng có tiền lệ trong lịch sử nước này". Cuộc tấn công đã làm toàn bộ hệ thống máy tính của Chính phủ Ukraina bị sập, hoạt động của hàng loạt ngân hàng, công ty của nước này bị gián đoạn. Một số máy tính của hệ thống cảm biến tại Nhà máy điện hạt nhân Chernobyl sử dụng hệ điều hành Windows cũng bị vô hiệu hóa, phải kiểm soát phóng xạ một cách thủ công. **Tại Nga**, nhiều ngân hàng, hàng chục hệ thống máy tính của các công ty lớn Nga bị mã độc tống tiền "Petya" tấn công, trong đó đáng chú ý là hệ thống máy tính của ngành khai khoáng Evraz, các máy chủ của hãng năng lượng Rosneft cũng đã bị ngưng trệ khiến Tập đoàn này đã phải chuyển sáng mạng quản lý và điều hành dự phòng đối với các quy trình sản xuất. Một số máy tính của các công ty thuộc tập đoàn lớn trên thế giới vận tải biển Maersk của Đan Mạch, tập đoàn quảng cáo WPP của Anh, tập đoàn công nghiệp Saint-Gobain của Pháp, 17 cảng Container của công ty APM tại Hà Lan, một công ty quốc tế lớn có chi nhánh tại Na Uy, hãng dược Merck, một bệnh viện tại Pittsburg và văn phòng tại Mỹ của hãng Luật DLA Piper cũng trở thành nạn nhân của cuộc tấn công bằng mã độc đòi tiền

chuộc Petya và Petrwrap (một biến thể cải tiến của Petya), làm một số hoạt động của hãng và chi nhánh bị ngưng trệ hoặc tê liệt.

2. Từ tình hình trên, Công an tỉnh – Cơ quan thường trực Ban Chỉ đạo bảo đảm an toàn thông tin mạng – Tỉnh ủy đề nghị các cơ quan, ban, ngành, địa phương tiến hành các biện pháp sau để chủ động phòng ngừa, ngăn chặn mã độc:

- Tiếp tục triển khai các biện pháp phòng ngừa theo Thông báo số 2342/TB-CAT-PA81 ngày 24/5/2017 về "hoạt động nguy hiểm của mã độc tống tiền Wannacry", khẩn trương cài đặt bản vá MS17-010 cho các máy tính và máy chủ của cơ quan, đơn vị.

- Để chủ động ngăn ngừa, ngăn chặn mã độc mã hóa dữ liệu, có thể tạo tập tin perfc tại đường dẫn "C:\Windows\perfc" và thiết lập thuộc tính chỉ đọc (read only), hoặc tải và thực thi tệp tin tại địa chỉ https://download.bleepingcomputer.com/bats/nopetyavac.bat.

- Đối với các cơ quan, đơn vị quản lý hệ thống mạng theo mô hình tập trung (domain), ngoài các biện pháp nêu trên, cần triển khai các biện pháp kỹ thuật siết chặt chính sách bảo mật theo hướng của Microsoft tại địa chỉ: https://www.microsoft.comen-us/download/details.aspx?id=36036" để ngăn chặn mã độc tấn công, kiểm soát toàn bộ hệ thống mạng.

- Trường hợp phát hiện mã độc Petya lây nhiễm vào hệ thống, đề nghị các cơ quan, đơn vị cô lập các máy tính bị lây nhiễm, thông báo về Công an (qua phòng An ninh Kinh tế, điện thoại (0234.3823966) để phối hợp ngăn chặn, xử lý.

Cơ quan thường trực an ninh mạng xin thông báo./.

Nơi nhận:
- Đ/c Bí thư Tỉnh ủy;
- Đc Chủ tịch UBND tỉnh;
- Đ/c Bùi Thanh Hà – PBT TT TU- Trưởng ban Chỉ đạo BĐATTTM.
- Các sở, ban ngành cấp tỉnh;
- Ngân hàng Nhà nước Việt Nam chi nhánh TT Huế;
- Cảng Hàng không Quốc tế Phú Bài;
- Công an các đơn vị, địa phương (để thực hiện);
- Lưu: VT, PA81(Đ1,Đ5).

GIÁM ĐỐC

CÔNG HÒA X.H.C.N VIỆT NAM
CÔNG AN TỈNH THỪA THIÊN

Đại tá Lê Quốc Hùng