**HƯỚNG DẪN PHÒNG CHỐNG BIẾN THỂ MỚI CỦA**

**RAMSOMWARE (MÃ ĐỘC PETYA)**

Ngày 28/06/2017 Cục an toàn thông tin (CATTT) công bố văn bản cảnh báo về biến thể mới của mã độc tống tiền Ramsomware (mã độc Petya).

Mã độc tống tiền, mã độc mã hóa dữ liệu (Ransomware) từ khi xuất hiện đã gây thiệt hại không nhỏ cho nhiều tổ chức, doanh nghiệp. Sau đợt tấn công hồi tháng 5 của mã độc tống tiền WannaCry, ngày 27/6/2017 mã độc Ransomware lại tiếp tục gây ảnh hưởng tới nhiều nước trên thế giới.

Biến thế mã độc lần này có tên Petya (còn gọi là Petwrap) không chỉ khai thác và lây lan thông qua lỗ hổng MS17-010 mà còn có thể lây nhiễm vào máy tính đã vá lỗ hổng này thông qua công cụ WMIC (công cụ có sẵn trong Windows cho phép truy cập và thiết lập cấu hình trên các máy Windows); công cụ PSEXE (công cụ cho phép truy cập vào máy tính Windows từ xa mà người dùng không biết thông qua dịch vụ SMB) và lỗ hổng CVE-2017-0199 (lỗ hổng trong Microsoft Office/WordPad cho phép tin tặc chiếm quyền điều khiển hệ thống).

Các lỗ hổng trên đã có bản vá, tuy nhiên có nhiều máy tính vẫn chưa cập nhật và có thế là nạn nhân của đợt tấn công lần này.

Petya có hoạt động rất khác so với các biến thể Ransomware khác. Petya khi lây nhiễm vào máy tính sẽ không mã hóa từng tập tin, mà thực hiện mã hóa Bảng File (Master File Table – MFT, chứa thông tin về tất cả các tập tin và thư mục trong phân vùng) và thay thế Master Boot Record của máy tính bằng tập tin độc hại để hiển thị thông tin đòi tiền chuộc. Do vậy máy tính người dùng sẽ không thể khởi động được khi bị nhiễm mã độc này.

Sở Thông tin và Truyền thông đề nghị các cơ quan, tổ chức tăng cường các biện pháp bảo đảm an toàn thông tin để giảm thiểu nguy cơ từ mã độc Petya như sau:

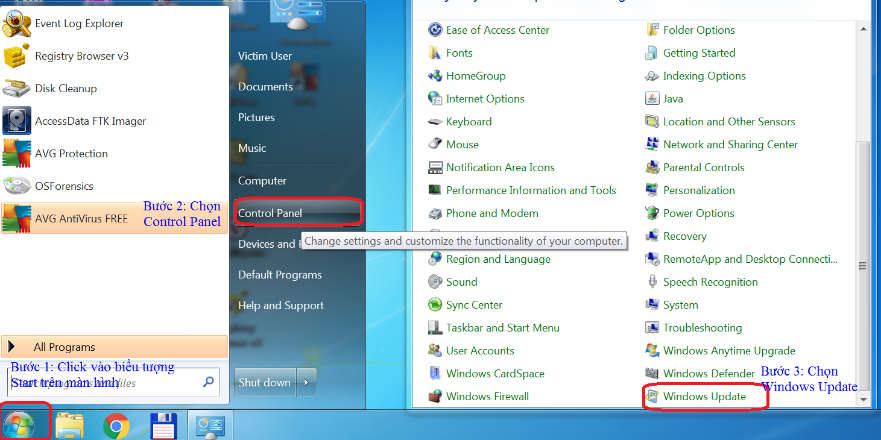
* Kiểm tra và đảm bảo các máy tính trong hệ thống mạng đã được cập nhật các lỗ hỏng bảo mật đặc biệt nghiêm trọng như: MS17-010, CVE 2017-0199.

**Hướng dẫn cách cập nhật hệ thống bằng Windows Update:**

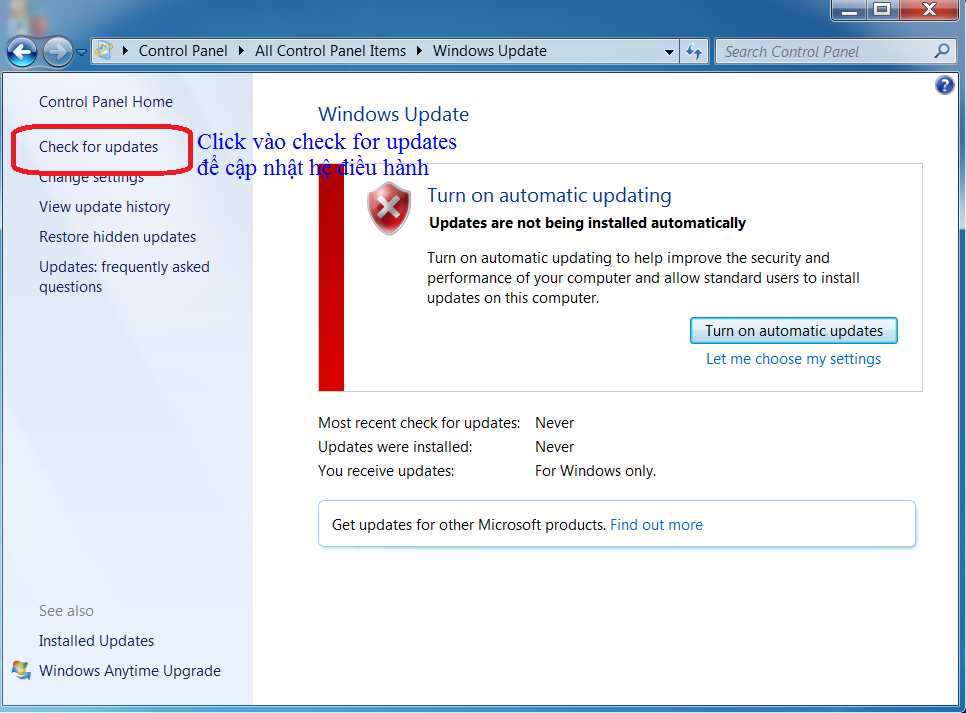
Thông thường, Windows Update sẽ tự động cập nhật hệ điều hành theo định kỳ, tuy nhiên, nếu bạn muốn kiểm tra và cập nhật ngay các nâng cấp mới nhất, bạn có thể tiến hành theo cách sau:

**Cách 1:** Vào "**Start Menu**" rồi mở "**Control Panel**"

Chọn mục "**System and Security**" rồi vào phần "**Windows Update**"



Bấm "**Check for Updates**" ở cột bên trái để tiến hành cập nhật hệ điều hành

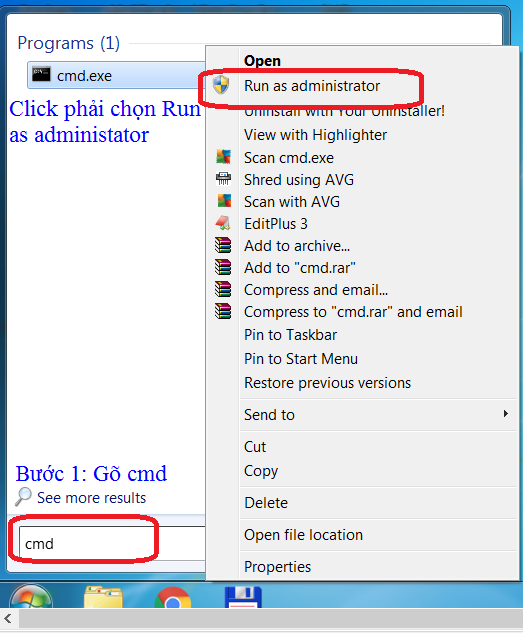


Sau khi đã thiết lập xong, bạn bấm "**OK**" để xác nhận thay đổi và quay về lại cửa sổ "**Windows Update**"

**Cách 2:** Dowload các bản cập nhật MS17-010, CVE 2017-0199 và cài trực tiếp vào máy. Click vào đường link <https://technet.microsoft.com/en-us/library/security/ms17-010.aspx> chọn đúng phiên bản hệ điều hành máy đang sử dụng thực hiện dowload về và cài đặt.

* Chặn toàn bộ kết nối liên quan đến dịch vụ SMB (445/137/138/139) bằng cách :

Vào “**Start Menu**” gõ **cmd** và chạy với quyền **Administrator (Run as administrator).**



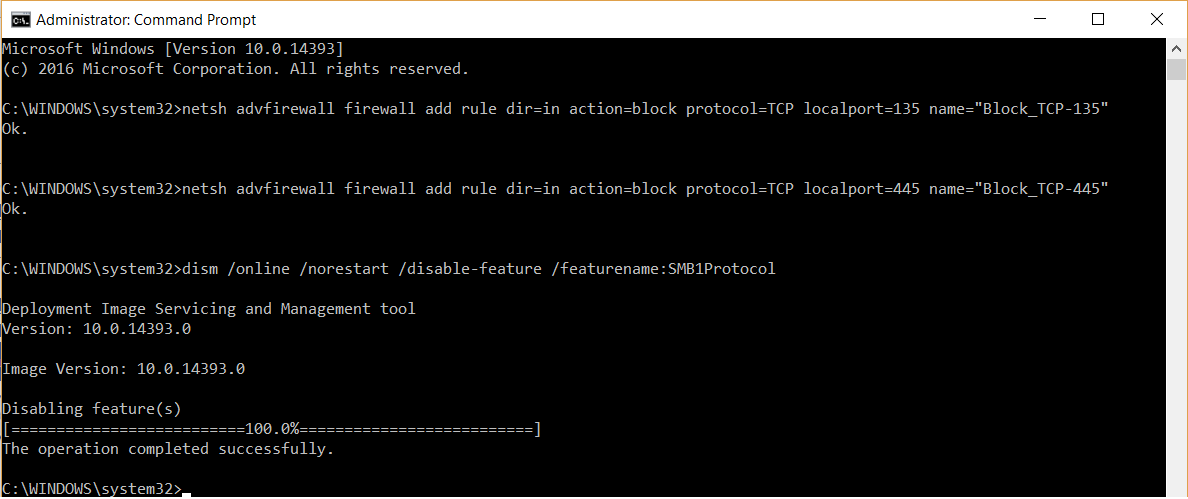
Sau đó nhập từng lệnh dưới đây vào cửa sổ Command Prompt (sau mỗi lệnh sẽ hiển thị trạng thái OK):

**netsh advfirewall firewall add rule dir=in action=block protocol=TCP localport=135 name="Block\_TCP-137"**

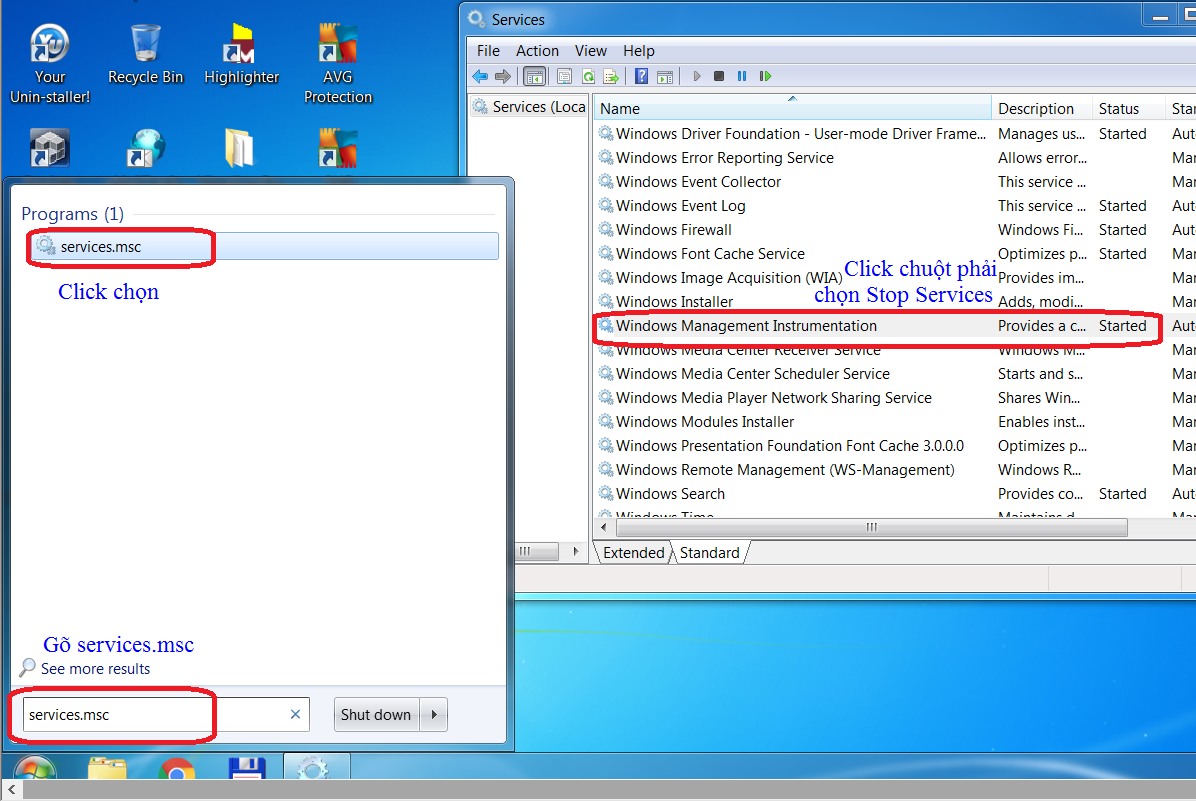
**netsh advfirewall firewall add rule dir=in action=block protocol=TCP localport=135 name="Block\_TCP-138"**

**netsh advfirewall firewall add rule dir=in action=block protocol=TCP localport=135 name="Block\_TCP-139"**

**netsh advfirewall firewall add rule dir=in action=block protocol=TCP localport=445 name="Block\_TCP-445"**



* Vô hiệu quá WMIC (Windows Management Instrumentation Command-line). Vào **Command Prompt** chọn Service.msc, khi hộp thoại service xuất hiện tìm service **Windows Management Instrumentation** click chuột phải chọn **Stop.**



Trong trường hợp cần thiết, Quý đơn vị có thể liên hệ với Sở Thông tin và Truyền thông, điện thoại: 0276 3611169, thư điện tử [hotro@tayninh.gov.vn](mailto:hotro@tayninh.gov.vn) để được phối hợp, hỗ trợ.