|  |  |  |  |
| --- | --- | --- | --- |
| BỘ THÔNG TIN VÀ TRUYỀN THÔNG  **TRUNG TÂM ỨNG CỨU KHẨN CẤP**  **MÁY TÍNH VIỆT NAM**  Số: /VNCERT-ĐPƯC  V/v theo dõi, ngăn chặn kết nối và xoá các tập tin chứa mã độc | **CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM**  **Độc lập - Tự do - Hạnh phúc**  *Hà Nội, ngày tháng năm 2016* |  |  |

Kính gửi:

* Các đơn vị chuyên trách về CNTT các Bộ, Ngành;
* Các Sở thông tin và Truyền thông;
* Thành viên mạng lưới ứng cứu sự cố Internet Việt Nam;
* Các tổ chức Tài chính, Ngân hàng.

Thực hiện Thông tư 27/2011/TT-BTTTT về điều phối các hoạt động ứng cứu sự cố mạng Internet Việt Nam, Trung tâm VNCERT yêu cầu Lãnh đạo đơn vị chỉ đạo các đơn vị thuộc phạm vi quản lý thực hiện khẩn cấp các việc:

1. Theo dõi và ngăn chặn kết nối đến các tên miền sau:

*a) playball.ddns.info*

*b) nvedia.ddns.info*

*c) air.dcsvn.org*

2. Rà quét hệ thống và xoá các thư mục và tập tin mã độc có kích thước tương ứng:

*a) C:\Program Files\Common Files\McAfee\McAfee.exe (137.28 KB)*

*- MD5: 884D46C01C762AD6DDD2759FD921BF71*

*- SHA-1: D201B130232E0EA411DAA23C1BA2892FE6468712*

*b) C:\Program Files\Common Files\McAfee\McUtil.dll (3.50 KB)*

*- MD5: C52464E9DF8B3D08FC612A0F11FE53B2*

*- SHA-1: E464D10AD93600232D7A24856D69F00510949A40*

*c) C:\Windows\system32\DiskMgers.dll (85.00 KB)*

*- MD5: 9BF793EF195CC62F8A61093F77B03158*

*- SHA-1: 46844B0ACF2BB67ADBF2304A61BE07738D2DDD64*

*d) Tập tin “diskperf.exe”: tìm tất cả các file trong ổ Hệ điều hành có:*

*- MD5: 29E656E1256FC998B7CE8494656B3EF8*

*- SHA-1: 8C073B63D85CBF48BD742A62C7A59EEB064DA74D*

3. Hướng dẫn kiểm tra mã MD5, SHA-1 của tập tin và cách thức xoá tập tin chữa mã độc trong Phụ lục kèm theo.

4. Sau khi thực hiện, yêu cầu các đơn vị báo cáo tình hình về Đầu mối điều phối ứng cứu sự cố quốc gia (Trung tâm VNCERT) theo địa chỉ email: ir@vncert.gov.vn / điện thoại: 0934424009 trước 16h ngày 05/8/2016.

5. Trên đây là những mã độc đặc biệt nguy hiểm, có thể đánh cắp thông tin và phá huỷ hệ thống, Trung tâm VNCERT yêu cầu Lãnh đạo các đơn vị nghiêm túc thực hiện lệnh điều phối.

Trân trọng./.

|  |  |
| --- | --- |
| ***Nơi nhận:***  - Như trên;  - Bộ trưởng Trương Minh Tuấn (để b/c);  - Thứ trưởng Nguyễn Thành Hưng (để b/c);  - Giám đốc (để b/c);  - Các chi nhánh, phòng: HCM, ĐN, KTHT;  - Lưu VT, ĐPƯC. | **KT.GIÁM ĐỐC**  **PHÓ GIÁM ĐỐC**  **Nguyễn Khắc Lịch** |

**PHỤ LỤC**

Hướng dẫn kiểm tra mã MD5, SHA-1 của tập tin và cách thức xoá tập tin

chứa mã độc

*(Kèm theo công văn số: /VNCERT-ĐPƯC ngày 03 tháng 8 năm 2016 của Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam)*

**1. Hướng dẫn kiểm tra mã hash MD5, SHA-1:**

a) Download phần mềm tại: http://www.nirsoft.net/utils/hashmyfiles.zip

b) Kiểm tra: Giải nén tập tin hashmyfiles.zip trên, tiến hành mở file “HashMyFiles.exe”. Nhấn vào File -> Add Files; Trỏ đến file cần kiểm tra mã Hash. Mã MD5 và SHA-1 sẽ hiển thị bên khung chương trình. Bạn chỉ cần đối chiếu mã MD5 và SHA-1 tương ứng trong Công văn đi kèm.

**2. Hướng dẫn gỡ bỏ tập tin chứa mã độc:**

a) Xác định mã độc: Nếu mã MD5 và SHA-1 trùng nhau thì tập tin trên máy tính là phần mềm có chứa mã độc. Nếu không trùng thì chưa khẳng định 100% nó không phải là mã độc. Có thể không xoá trong trường hợp này.

b) Cách xoá tập tin chứa mã độc: Do tập tin này đang chạy nên ta cần dừng hoặc tắt tiến trình này trước khi xoá. Trước tiên cần tải phần mềm miễn phí có tên “Process Explorer” của Microsoft tại địa chỉ bên dưới: <https://download.sysinternals.com/files/ProcessExplorer.zip>

Sau khi tải về giải nén ta chạy file “procexp.exe”. Tiến hành tìm kiếm các tiến trình tương ứng trong Công văn ở trên và nhấn chuột phải chọn “Suspend” hoặc “Kill Process”. Sau khi chọn xong, ta vào đường dẫn tương ứng để xoá.