BỘ THÔNG TIN VÀ TRUYỀN THÔNG
CỤC AN TOÀN THÔNG TIN

Số: 143/CATTT-NCSC
V/v Cảnh báo tấn công mạng thông qua dịch vụ Remote Desktop vào các máy chủ của Việt Nam

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

Hà Nội, ngày 20 tháng 02 năm 2019

Kính gửi:

- Đơn vị chuyên trách về CNTT các bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ;
- Sở Thông tin và truyền thông các tỉnh, thành phố trực thuộc Trung ương;
- Các Tập đoàn, Tổng công ty nhà nước; Các Ngân hàng TMCP; Các tổ chức tài chính.

Hiện nay đang có một chiến dịch tấn công vào các máy chủ tại Việt Nam. Tất cả các máy chủ tại Việt Nam đang **mở cổng Remote Desktop** đều là mục tiêu tấn công. Hình thức tấn công là dò quét mật khẩu quản trị trên các máy chủ, nếu phát hiện tài khoản quản trị trên máy chủ sử dụng mật khẩu yếu, đối tượng tấn công sẽ thực hiện đăng nhập vào máy chủ và cài cắm mã độc **Mã hóa dữ liệu tống tiền** lên máy chủ. Chiến dịch tấn công này chủ yếu nhằm vào máy chủ để mã hoá dữ liệu trên máy chủ. Đối tượng tấn công đã và đang mở rộng chiến dịch tấn công với đích nhằm tới là các máy chủ trên toàn quốc, trong đó có cả cơ quan, tổ chức nhà nước.

Theo thông tin giám sát thu thập được, Việt Nam hiện tại có ít nhất **18.943** máy chủ đang mở cổng dịch vụ Remote Desktop. Nhằm bảo đảm an toàn thông tin, phòng tránh nguy cơ trở thành mục tiêu của chiến dịch này Cục An toàn thông tin (Cục ATTT) khuyến nghị:

(1) Rà soát toàn bộ máy chủ của đơn vị, hạn chế tối đa việc mở cổng dịch vụ Remote Desktop. Trong trường hợp cần sử dụng phải thiết lập các chính sách bảo mật như: sử dụng VPN, giới hạn IP truy cập, tài khoản được phép truy cập, chính sách mật khẩu mạnh (mật khẩu có tối thiểu 8 ký tự, có đầy đủ chữ hoa, chữ thường, số và ký tự đặc biệt). *Tham khảo hướng dẫn tại tài liệu kèm theo.*

(2) Sao lưu dữ liệu quan trọng trên máy chủ;

(3) Theo dõi, giám sát hệ thống để phát hiện sớm, kịp thời phản ứng các hành vi dò quét/tấn công mạng.

(4) Khi phát hiện bị tấn công mã hoá dữ liệu liên hệ với đơn vị cung cấp dịch vụ bảo mật/giải mã dữ liệu gần nhất để có biện pháp khôi phục dữ liệu.

Trong trường hợp cần thiết, có thể liên hệ Trung tâm Giám sát an toàn không gian mạng quốc gia thuộc Cục ATTT, số điện thoại: 024.3209.1616, thư điện tử ais@mic.gov.vn hoặc fanpage của NCSC theo đường dẫn https://www.facebook.com/govSOC/ để được hỗ trợ kịp thời.

Trân trọng./.

Nơi nhận:
- Như trên;
- Lãnh đạo Bộ (để b/c);
- Cục trưởng (để b/c);
- Lưu: VT, NCSC.

KT. CỤC TRƯỞNG
PHÓ CỤC TRƯỞNG

CỘNG HÒA X.H.C.N VIỆT NAM
CỤC AN TOÀN THÔNG TIN
BỘ THÔNG TIN VÀ TRUYỀN THÔNG

Nguyễn Huy Dũng

HƯỚNG DẪN ĐẢM BẢO AN TOÀN KHI QUẢN TRỊ TỪ XA DÙNG REMOTE DESKTOP

1. Sử dụng tên toàn khoản và mật khẩu mạnh

Thay vì đặt tên tài khoản là tên bản thân, bạn bè, gia đình thú cưng… Hoặc những tài khoản mặc định như Admin thì hãy đổi tên tài khoản khác.

Khi sử dụng mật khẩu, cần đặt mật khẩu :

- Chứa 8 ký tự trở lên;

- Chứa các ký tự từ 2 trong 3 trường ký tự như sau :

+ Bằng chữ cái (ví dụ: a->z, A->Z)

+ Số (0->9)

+ Các ký tự đặc biệt (:! @ # $% ^ & * () _ + | ~ - = \ ` {} []:"; '<>?,. /)

- Mật khẩu không nên bao gồm:

+ Tên username

+ Các cụm từ xuất hiện trong từ điển

+ Đánh vần ngược

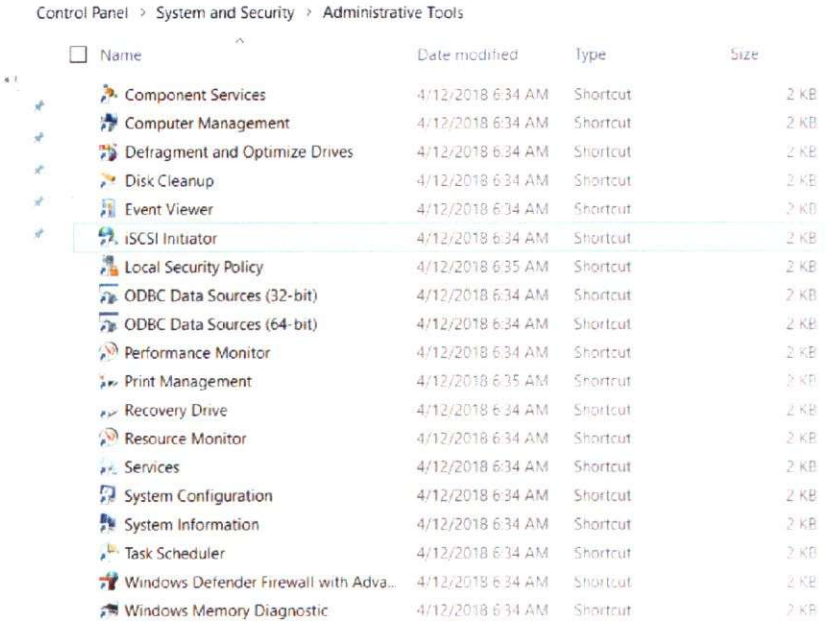
2. Giới hạn số lần đặng nhập sai

Các cuộc tấn công RDP cần phải dùng hàng ngàn, triệu lần đặng nhập liên tục. Vì vậy có thể tăng thời để thực hiện tấn công lên rất nhiều lần thì nên khóa người dùng sau một số lần đăng nhập sai nhất định trong 1 khoảng thời gian nhất định

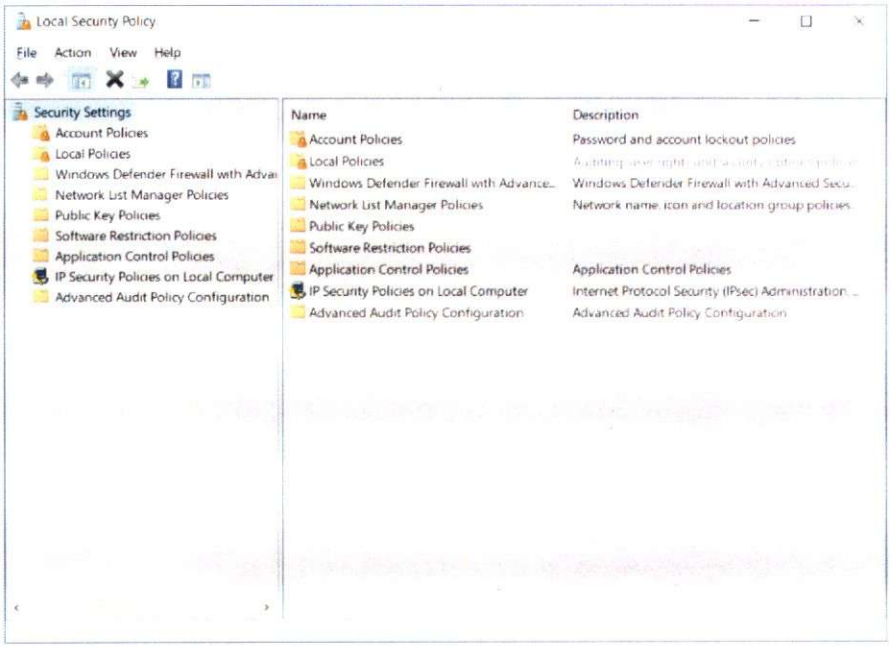
Cách thiết lập giới hạn:

Mở Administrative Tools

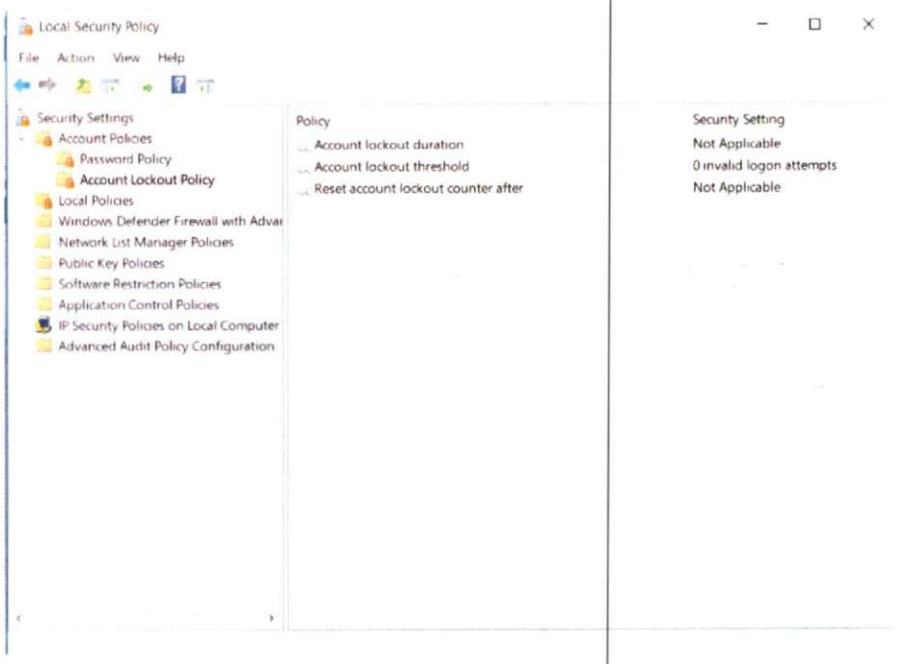
- Control panel -> System and Security -> Administrative Tools



- Mở **Local Security Policy**



- Mở tab **Account Policies** rồi bên trong mở tab **Account Lockout Policy**



- Kích hoạt giới hạn ở phần **Account Lockout Threshold**

- Chỉnh thời gian khóa tại tab **Account Lockout Duration**

3. Thay đổi cổng RDP

- Khi quét, Hacker thường tìm kiếm các kết nối sử dụng cổng RDP mặc định (TCP 3389). Chúng ta có thể ẩn các kết nối RDP của mình bằng cách thay đổi công sang cổng khác. Tuy nhiên cần lưu ý tránh xung đột cổng kết nối với phần mềm khác (như cổng 80 – HTTP , cổng 443 – HTTPS …)

- Cách thực hiện:

+ Vào **Start**, chọn **Run** (hoặc bấm phím **Windows + R**)

+ Tìm đến đường dẫn:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp