BỘ KHOA HỌC VÀ CÔNG NGHỆ
TRUNG TÂM CÔNG NGHỆ THÔNG TIN

Số: 40 /CV-TTCNTT
V/v Cảnh báo tấn công mạng thông qua dịch vụ Remote Desktop và tấn công APT

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

Hà Nội, ngày 25 tháng 02 năm 2019

Kính gửi:

Theo thông tin từ Cục An toàn thông tin – Bộ Thông tin và Truyền thông, đang có một chiến dịch tấn công nhằm 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 của hacker. Hình thức tấn công là dò 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 của nạn nhân. Chiến dịch tấn công này chủ yếu nhằm vào máy chủ để mã hóa dữ liệu trên máy chủ. Đối tượng tấn công đã mở rộng chiến dịch tấn công và đích nhằm tới là các máy chủ trên toàn quốc, trong đó có cả cơ quan, tổ chức nhà nước.

Ngoài ra, Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam (VNCERT) đã ghi nhận chiến dịch tấn công có chủ đích (APT) của tin tặc nhằm vào các hệ thống thông tin của ngân hàng và tổ chức chủ quản hệ thống thống tin hạ tầng quan trọng quốc gia tại Việt Nam. Mục đích chính của tin tặc là đánh cắp các thông tin quan trọng của hệ thống thông tin của ngân hàng và tổ chức chủ quản hệ thống thống tin hạ tầng quan trọng quốc gia. Với việc sử dụng các kỹ thuật cao để tấn công thì các hệ thống bảo vệ ATTT của hệ thống thông tin của ngân hàng và tổ chức chủ quản hệ thống thống tin hạ tầng quan trọng quốc gia sẽ khó phát hiện kịp thời và đồng thời giúp tin tặc duy trì quyền kiểm soát hệ thống thông tin.

Nhằm bảo đảm an toàn thông tin, phòng tránh nguy cơ trở thành mục tiêu của các chiến dịch nêu trên Trung tâm Công nghệ thông tin đề nghị:

1. Theo dõi và ngăn chặn kết nối đến các máy chủ C&C có tên miền và địa chỉ IP sau:

STT	C&C	STT	C&C
1	192.227.248.189	27	192.227.248.188
2	usfinance.club	28	107.175.75.115
3	ukfinance.online	29	zzivet37.pro
4	107.174.39.144	30	wvideo.site
5	184.164.139.212	31	usfinance.store
6	shengu.tech	32	107.175.64.217
7	kalya.website	33	pixeliph.com
8	smtp3.info	34	198.46.209.171
9	urlmon.online	35	108.170.60.181

10	107.175.94.16	36	62.255.119.211
11	zivet37.services	37	192.95.14.128
12	gpcantgua.com	38	kair.xyz
13	107.172.3.16	39	autoif.online
14	107.175.75.116	40	crossfr.site
15	167.114.56.226	41	dochelp.space
16	66.85.157.69	42	185.136.165.202
17	107.172.249.103	43	107.172.249.122
18	198.46.168.33	44	198.23.140.75
19	172.245.205.107	45	107.172.150.141
20	167.114.56.224	46	185.136.163.167
21	116.197.235.202	47	151.106.60.15
22	72.83.72.137	48	198.46.168.29
23	vanxuangroup.edu.vn	49	151.106.60.136
24	gpcantgua.com	50	192.227.248.181
25	192.64.119.21	51	192.64.119.87
26	192.64.119.20	52	192.64.119.86

2. Rà quét hệ thống, xóa các thư mục và bóc gỡ tập tin mã độc có dấu hiệu tương ứng sau:

- MD5: 25376ea6ea0903084c45bf9c57bd6e4f
- MD5: 1e2795f69e07e430d9e5641d3c07f41e
- MD5: 3be75036010f1f2102b6ce09a9299bca
- HSMBalance.exe MD5: 34404a3fb9804977c6ab86cb991fb130
- HSMBalance.exe SHA-1:b345e6fae155bfaf79c67b38cf488bb17d5be56d
- ICAS.ps1 MD5: b12325a1e6379b213d35def383da2986
- ICAS.ps1 SHA-1: c48ff39e5efc6ca60c31200344c47b5de3b3605d
- MD5: 7c651d115109fd8f35fdfc44fd24518
- MD5: 8a41520c89dce75a345ab20ee352fef0
- MD5: b88d4d72fdabfc040ac7fb768bf72dcd
- hs.exe MD5: df934e2d23507a7f413580eae11bb7dc
- hs.exe SHA-1:5ce51e3882c40961caf2317a3209831ed77c9c40
- MD5: fee0b31cc956f083221cb6e80735fcc5
- MD5: 4c400910031ee3f12d9958d749fa54d5
- MD5: 2e0d13266b45024153396f002e882f15
- MD5: 26f09267d0ec0d339e70561a610fb1fd

- MD5: 09e4f724e73fccc1f659b8a46bfa7184
- MD5: 18c2adfc214c5b20baf483d09c1e1824
- MD5: 2cd8e5d871f5d6c1a8d88b1fb7372eb0
- MD5: e9130a2551dd030e3c0d7bb48544aaea
- MD5: 9888d1109d6d52e971a3a3177773efaa
- MD5: be021d903653aa4b2d4b99f3dbc986f0
- MD5: 2036a9e008d16e8ac35614946034b1a5
- MD5: ef5741c4b96ef9498357dc4d33498163
- MD5: 5B7244C47104F169B0840440CDEDE788
- MD5: 53F7BE945D5755BB628EECB71CDCBF2
- MD5: E00499E21F9DC990400B8B3C2B5
- MD5: 9c35e9aa9255a2214d704668b039ef6
- MD5: cc29adb5b78300b0f17e566ad461b2c7
- MD5: C6774C1417BE2E8B7D14BAD1391|1DO4B

3. 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.*

4. Sao lưu dữ liệu quan trọng trên máy chủ;

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

6. Khi phát hiện bị tấn công mã hóa dữ liệu liên hệ với đơn vị cung cấp dịch vụ bảo mật/giải mã dữ liệu chuyên nghiệp để có biện pháp khôi phục dữ liệu.

7. Sau khi theo dõi, ngăn chặn kết nối đến các máy chủ C&C và rà quét hệ thống, bóc gỡ các tập tin mã độc (nếu có), đề nghị các đơn vị báo cáo kết quả về Phòng Kỹ thuật hạ tầng – Trung tâm Công nghệ thông tin theo địa chỉ thư điện tử phongktht@most.gov.vn / số điện thoại: 024.39439060 **trước ngày** 04/03/**2019**.

Trân trọng./.

Nơi nhận:
- Như trên;
- Thứ trưởng Bùi Thế Duy (để b/c);
- Lưu: TTCNTT.

GIÁM ĐỐC

TRUNG TÂM CÔNG NGHỆ THÔNG TIN

Hà Quốc Trung

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

1. Sử dụng tên toàn khoản và mật khẩu mạnh

Không sử dụng tài khoản mặc định như: admin, administrator…

Khi sử dụng mật khẩu, cần đặt mật khẩu như sau:

- Có tối thiểu 8 ký tự;
- Có đầy đủ chữ hoa, chữ thường, số và ký tự đặc biệt:
  + Bẳng 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

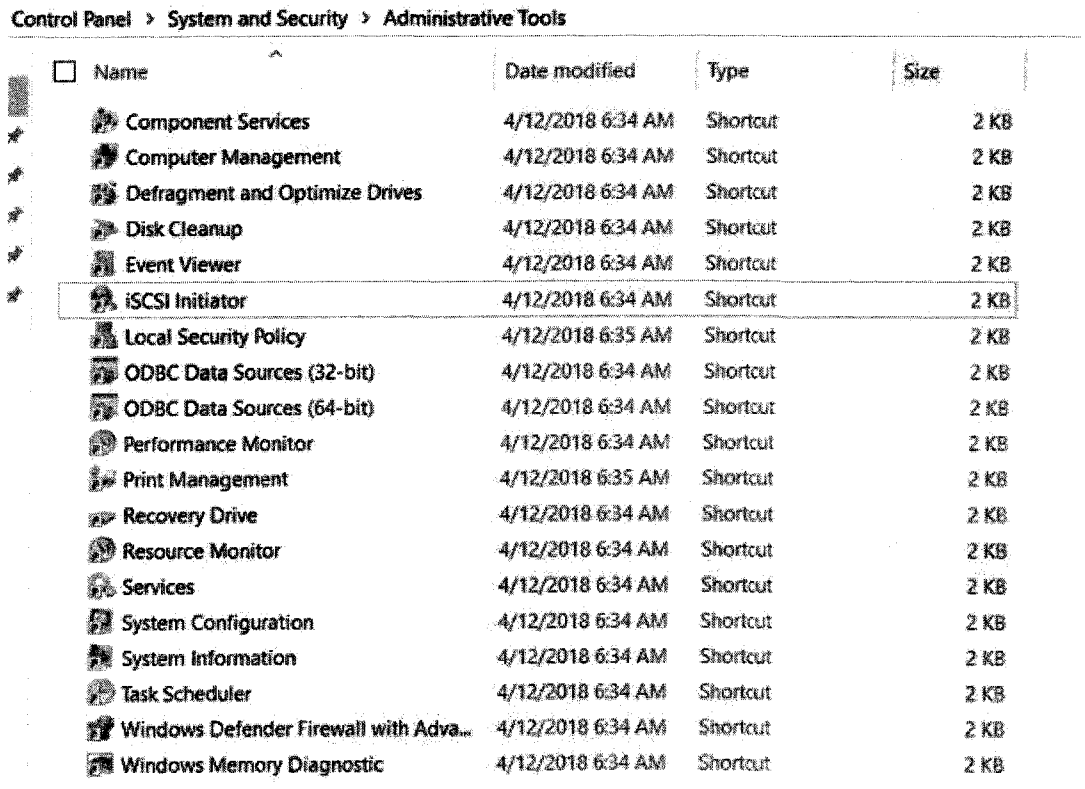
2. Giới hạn số lần đăng nhập sai

Các cuộc tấn công RDP cần phải dùng hàng ngàn, triệu lần đăng nhập liên tục. Vì vậy có thể tăng thời gian 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.

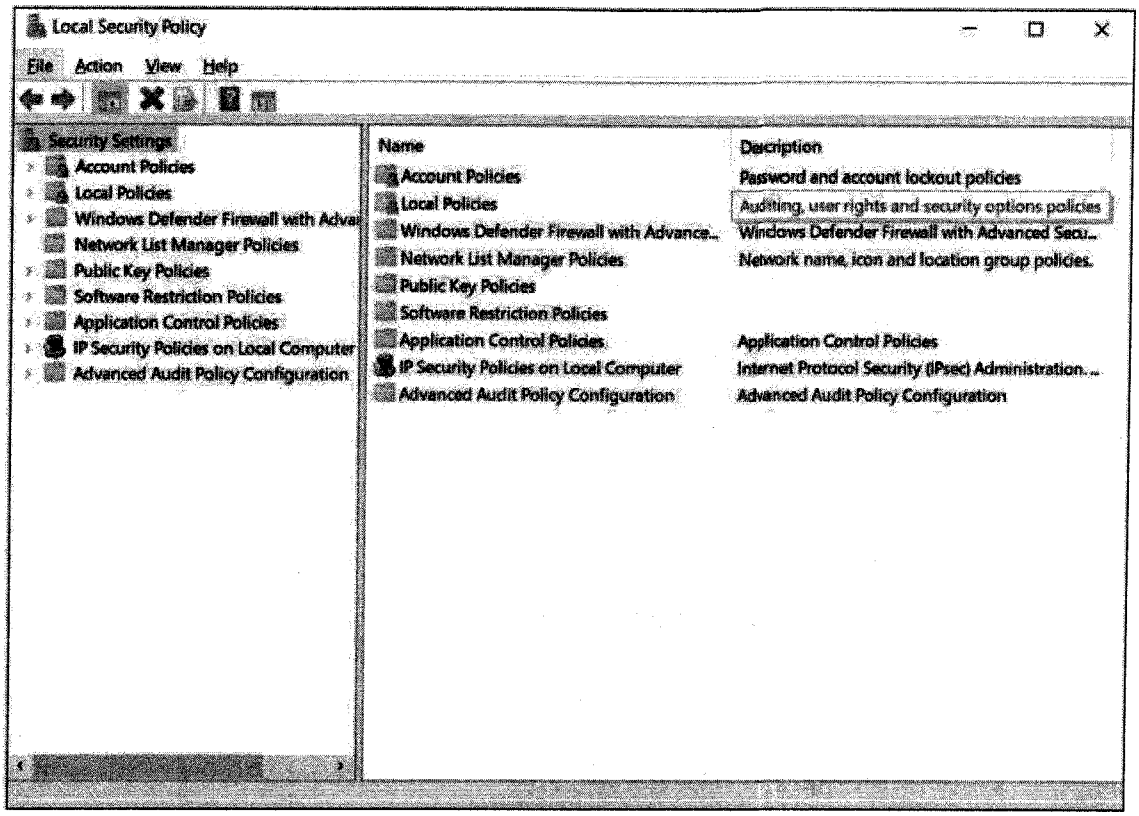
Cách thiết lập giới hạn:

Mở Administrative Tools

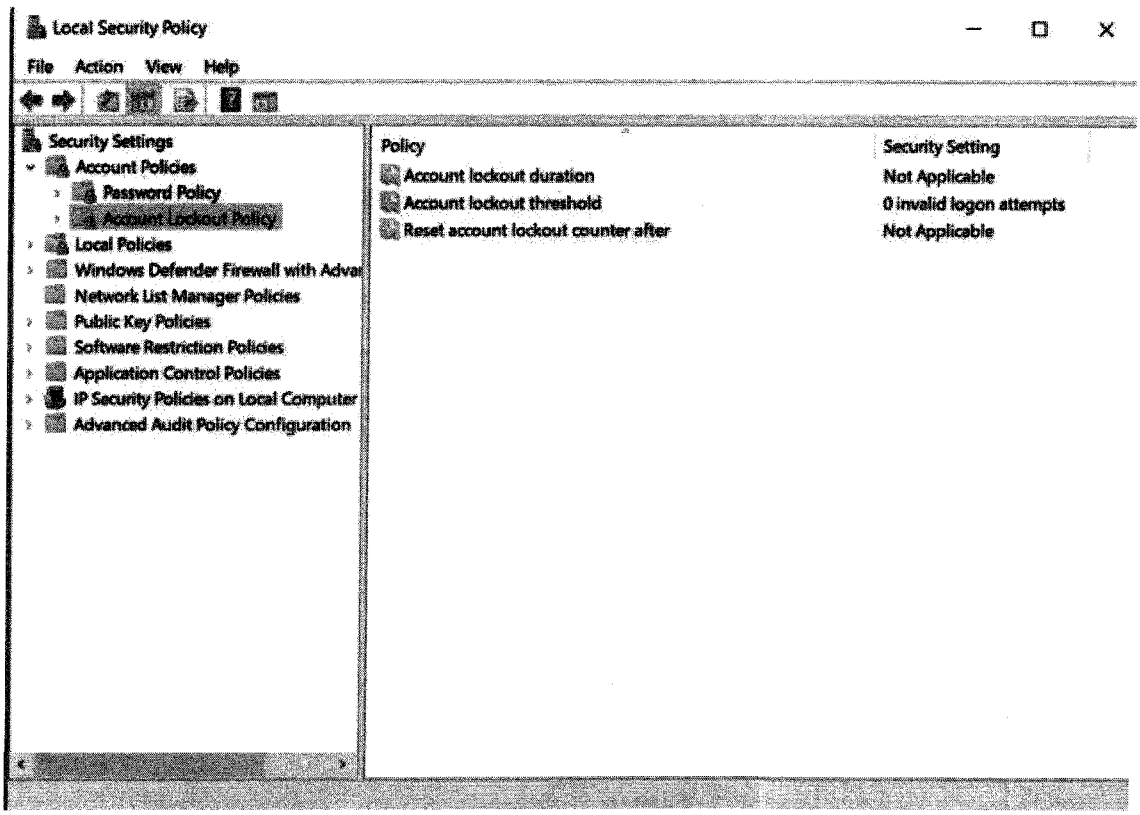
- Control panel -> System and Security -> Administrative Tools



- 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). Cán bộ quản trị có thể ẩn các kết nối RDP 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 …)

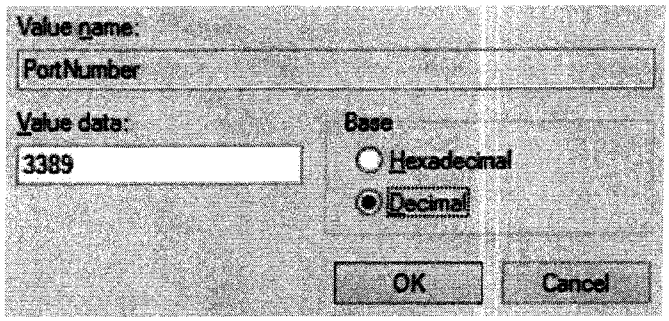
- Cách thực hiện:

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

+ Tìm đến đường dẫn:

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

Click đúp vào PortNumber và chọn Decimal sau đó nhập vào số port cần thay đổi ở mục Value data:



4. Triển khai giải pháp bảo đảm an toàn khi truy cập từ xa

- Nếu cần truy cập quản trị server từ xa dùng Remote Desktop, ưu tiên sử dụng kênh kết nối VPN

- Kênh kết nối VPN có thể triển khai trên các hệ thống Windows Server hoặc các thiết bị Firewall chuyên dụng.