ỦY BAN NHÂN DÂN TỈNH ĐỒNG THÁP	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 410 /UBND-TCD-NC Về việc ngăn chặn hoạt động tấn công mạng, rà soát, gỡ bỏ mã độc của các nhóm tin tặc nước ngoài tại Việt Nam	*Đồng Tháp, ngày 23 tháng 7 năm 2021*

Kính gửi:
- Các sở, ngành Tỉnh;
- Ủy ban nhân dân huyện, thành phố.

Theo thông báo của Bộ Công an: Trong 06 tháng đầu năm 2021, đã phát hiện 04 nhóm tin tặc nước ngoài tăng cường khai thác các điểm yếu, lỗ hổng bảo mật và việc không chấp hành các quy định về bảo vệ bí mật nhà nước trong quản lý, vận hành hệ thống thông tin của các cơ quan, bộ, ngành, tổ chức, doanh nghiệp, để thực hiện tấn công mạng tại Việt Nam, nguy cơ gây mất an ninh mạng, an toàn thông tin. *Về phương thức, thủ đoạn và các dòng mã độc do các nhóm tin tặc nước ngoài sử dụng tại Việt Nam chủ yếu như sau:*

(1) Nhóm Goblin Panda: Sử dụng kỹ thuật tấn công "DLL Side-loading"[1], khai thác các lỗ hổng bảo mật trên bộ phần mềm Microsoft Office, tấn công "phishing" qua thư điện tử[2]. Đáng chú ý, gần đây, nhóm Goblin Panda đã nâng cấp, phát triển 02 dòng mã độc mới: "FoundCore" và "DropPhone" với các tập tin mã độc gồm: "outlib.dll", "rdmin.src" và các tài liệu, văn bản bị gắn mã độc: "QUAN HỆ MỸ TRUNG NĂM 2020 VÀ XU HƯỚNG THỜI GIAN TỚI.docx", "Nhungdiemmoinoibat_DuthaobaocaoDHXIII.docx"…

(2) Nhóm Mustang Panda: Sử dụng kỹ thuật tấn công "DLL Side-loading" với dòng mã độc "PlugX" và các biến thể nguy hiểm có tính năng lây nhiễm từ thiết bị lưu trữ bên ngoài (USB, đĩa CD định dạng "Like a USB flash drive") vào máy tính và ngược lại để thu thập, chiếm đoạt thông tin, tài liệu từ hệ thống mạng nội bộ; mã hóa, lưu trữ trong thư mục ẩn; khi có kết nối Internet, mã độc sẽ kết nối máy chủ điều khiển tại nước ngoài, để chuyển thông tin, tài liệu thu thập được đến kho lưu trữ của tin tặc. Các tập tin mã độc gồm: "audobeupdate", "http_dll.dat", "AvastAuth.dat", "AvastGuide.dat", "pdvdlib.dat", "hex.dll", "wsc.dll", "dllmain.dll", "BoomerangLib.dll", "HT.dll" *(có Phụ lục 1 kèm theo)*. Đặc biệt nguy hiểm, qua kiểm tra, rà soát, Bộ Công an phát hiện mã độc Mustang Panda đã lây nhiễm vào hệ thống mạng của nhiều cơ quan, bộ, ngành, địa phương, nguy cơ lộ, mất tài liệu nội bộ, tài liệu bí mật nhà nước.

(3) Nhóm FunnyDream: Khai thác lỗ hổng bảo mật trên hệ thống thông tin công khai trên mạng Internet *(tập trung chính vào các trang web)* để cài cắm, phát tán mã độc có tính năng do thám, thực thi lệnh từ xa và đánh cắp thông tin, tài liệu. Tập tin mã độc: "avp.dll".

---

[1] Giả mạo tập tin thư viện ".dll" của các ứng dụng, phần mềm hợp lệ trên máy tính bằng các tập tin chứa mã độc.
[2] Gửi đính kèm tập tin mồi nhử có nội dung thu hút chú ý để lừa nạn nhân mở, kích hoạt mã độc trên máy tính.

(4) Nhóm HAFNUM: Khai thác các lỗ hổng bảo mật "zero-day" trên các máy chủ thư điện tử sử dụng giải pháp Microsoft Exchange[3], sau đó sử dụng mã độc "ChinaChopper" để do thám, thực thi lệnh từ xa, tạo các "cửa hậu" cho phép chiếm đoạt dữ liệu và kiểm soát hệ thống. Các tập tin mã độc gồm: "App_Web_3dm0hqcd.dll", "segoeui-semilight.aspx.ec688436.compiled".

Ngoài ra, phát hiện và thu thập các tập tin mã độc nguy hiểm khác có tính năng do thám, đánh cắp thông tin người dùng và gửi trực tiếp về email hoặc tài khoản Telegram của tin tặc, gồm: "goopdate.dll" (Mimikatz); "crss.exe" (Glupteba); "sacrv.dll", "wbemimg.dll" (HttpShadowSever); "adobe_flash-update.exe" (Pylogger); "AMZ Manager 2.0.5.exe", "DeviceId.exe", "Namesis.rar", "loader.exe" (TelegramInfoStealer),…

Lỗ hổng bảo mật CVE-2021-1675 (còn gọi là PrintNightmare) tồn tại trong Windows Print Spooler (một quá trình quản lý, xử lý tác vụ in, fax và tương tác với máy in trong Windows, tập tin thực thi được đặt tên là spoolsv.exe), ảnh hưởng đến khoảng 40 phiên bản của hệ điều hành Windows *(Phụ lục 2 kèm theo)*. Khai thác lỗ hổng bảo mật này, tin tặc có thể: tấn công, chiếm quyền điều khiển đối với các máy tính, máy chủ sử dụng phiên bản Windows tồn tại lỗ hổng bảo mật; sử dụng tài khoản người dùng đã xác thực dịch vụ để tấn công leo thang đặc quyền (LPE) thông qua máy tính trong hệ thống mạng, chiếm quyền điều khiển đối với toàn bộ hệ thống; thực thi các đoạn mã độc từ xa (RCE). Đáng chú ý, lợi dụng lỗ hổng dịch vụ này, tin tặc phát tán vũ khí mạng Stuxnet lây nhiễm vào ít nhất 14 cơ sở công nghiệp, phá hủy hạ tầng công nghiệp.

Nhằm tăng cường bảo đảm an ninh mạng, an toàn thông tin trên địa bàn Tỉnh trong thời gian tới, Ủy ban nhân dân Tỉnh yêu cầu các sở, ngành Tỉnh, Ủy ban nhân dân huyện, thành phố thực hiện các nội dung sau:

1. Tiếp tục thực hiện nghiêm Chỉ thị số 02/CT-TTg ngày 04 tháng 7 năm 2018 của Thủ tướng Chính phủ về công tác bảo vệ bảo vệ bí mật nhà nước trên không gian mạng và Chỉ thị số 14/CT-TTg ngày 25 tháng 5 năm 2018 của Thủ tướng Chính phủ về nâng cao năng lực phòng, chống phần mềm độc hại.

2. Rà soát, khắc phục sơ hở, thiếu sót trong công tác quản lý, vận hành, sử dụng hệ thống mạng của các đơn vị, địa phương; đồng thời tổ chức quán triệt, chấp hành nghiêm các quy định của pháp luật về bảo vệ bí mật nhà nước.

3. Tổ chức rà soát, khắc phục lỗ hổng bảo mật, gỡ bỏ mã độc trên hệ thống mạng; thiết lập giám sát, ngăn chặn kết nối đến các máy chủ điều khiển mã độc; dừng dịch vụ Windows Print Spooler trên máy trạm, máy chủ trong hệ thống mạng không cần thiết và tiến hành cập nhật bản vá bảo mật cho các trang thiết bị *(có Phụ lục 3, 4, 5, 6 kèm theo).*

Kết quả kiểm tra, rà soát, ngăn chặn, bóc gỡ mã độc đề nghị trao đổi bằng văn bản gửi về Ủy ban nhân dân Tỉnh (qua Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao - Công an Tỉnh) **trước ngày 28 tháng 7 năm 2021.**

---

[3] Đơn vị chức năng của Bộ Công an đã có thông tin cảnh báo từ tháng 3 năm 2021.

Quá trình thực hiện, nếu có phát sinh khó khăn, vướng mắc kịp thời báo cáo về Ủy ban nhân dân Tỉnh (qua Công an Tỉnh) để được hướng dẫn xử lý./.

Nơi nhận:
- Như trên;
- TT/TU, TT/HĐND Tỉnh;
- CT, PCT/UBND Tỉnh;
- Lãnh đạo VP/UBND Tỉnh;
- Công an Tỉnh;
- Lưu: VT, TCD-NC(CT).

TM. ỦY BAN NHÂN DÂN
CHỦ TỊCH

Phạm Thiện Nghĩa