BỘ CÔNG AN
CÔNG AN TỈNH LẠNG SƠN

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

Số: 113 /CAT-PA05

Lạng Sơn, ngày 12 tháng 01 năm 2026

V/v cảnh báo thủ đoạn của các đối tượng tấn công xâm nhập hệ thống camera giám sát

Kính gửi: - Các sở, ban, ngành, đoàn thể;
- Đảng ủy, UBND các xã phường tỉnh Lạng Sơn.

Thời gian gần đây trên không gian mạng tán phát nhiều video clip nhạy cảm lộ lọt từ hệ thống camera giám sát (*điển hình là vụ việc hacker rao bán trên mạng xã hội X và telegramm gói dữ liệu chứa 4500 video clip nhạy cảm của hộ gia đình người dân Hàn Quốc được hack từ camera, vụ lộ video 'nhạy cảm' qua camera phòng làm việc tại trường học ở Ninh Bình)*. Tình hình trên cho thấy hoạt động tấn công xâm nhập hệ thống camera giám sát của các đối tượng tin tặc nhằm đánh cắp dữ liệu cá nhân, thông tin nội bộ của các cơ quan, tổ chức để trục lợi, phát tán và thực hiện đang diễn biến phức tạp. Các đối tượng không chỉ dừng lại ở hành vi xâm phạm bí mật đời tư, thu thập thông tin nhạy cảm của các cơ quan, tổ chức mà còn sử dụng dữ liệu này để thực hiện các hoạt động gián điệp mạng, xâm phạm đến quyền và lợi ích hợp pháp của các cơ quan, tổ chức, cá nhân, lưu hành văn hóa phẩm đồi trụy, cưỡng đoạt tài sản, bôi nhọ danh dự, nhân phẩm của công dân, gây bức xúc trong dư luận và ảnh hưởng xấu đến tình hình trật tự xã hội.

Một số phương thức thủ đoạn thường được các đối tượng sử dụng:

- *Khai thác lỗ hổng bảo mật:* Đối tượng sử dụng các công cụ rà quét IP, cổng (port) camera mở công khai trên internet (Shodan, Censys,...); Không giới hạn IP truy cập từ bên ngoài; Sử dụng dịch vụ xem từ xa nhưng cấu hình bảo mật kém.

- *Tấn công Brute-force:* Lợi dụng thói quen đặt mật khẩu mặc định, mật khẩu yếu hoặc không đổi mật khẩu của người dùng, nhà cung cấp dich vụ để xâm nhập trái phép;

- *Tấn công giả mạo (phishing, social engineering):* Lừa quản trị viên cung cấp tài khoản đăng nhập; Giả mạo email, tin nhắn từ nhà cung cấp hoặc bộ phận công nghệ thông tin.

- *Xâm nhập qua phần mềm quản lý camera:* Phần mềm xem/điều khiển camera trên máy tính có lỗ hổng; Máy tính quản trị bị nhiễm mã độc dẫn đến mất quyền kiểm soát camera.

- *Cài mã độc hoặc backdoor:* Firmware bị cài cửa hậu ngay từ đầu (tại chuỗi cung ứng); Thiết bị bị nhiễm mã độc khi cập nhật từ nguồn không tin cậy; Camera trở thành công cụ gián điệp hoặc botnet.

- *Lợi dụng camera làm điểm trung gian tấn công:* Camera bị chiếm quyền điều khiển trở thành "bàn đạp"; từ camera, kẻ tấn công mở rộng sang máy chủ và hệ thống khác và khó phát hiện vì camera thường ít được giám sát an ninh.

- *Kinh doanh trái phép dữ liệu hoặc thực hiện các hoạt động gián điệp mạng:* Sau khi chiếm đoạt quyền điều kiển, đối tượng trích xuất các đoạn video nhạy cảm, thu thập các thông tin, dữ liệu để rao bán hoặc tiến hành các hoạt động gián điệp mạng sâu hơn đối với các cơ quan, tổ chức như: Thu thập thông tin tình báo bí mật, xâm nhập sâu vào hệ thống mạng nội bộ, nghe lén và thu âm trái phép,…

Để phòng ngừa, ngăn chặn và phối hợp đấu tranh có hiệu quả với tội phạm tấn công, xâm nhập hệ thống camera giám sát đánh cắp dữ liệu, Công an tỉnh Lạng Sơn đề nghị:

1. Thủ trưởng các sở, ban, ngành, đoàn thể, Đảng ủy, UBND các xã, phường quan tâm chỉ đạo, tăng cường tuyên truyền bằng nhiều hình thức đến cán bộ, đảng viên, nhân dân để nâng cao nhận thức về an ninh mạng và an toàn thông tin, cảnh giác tránh rơi vào bẫy của các đối tượng tấn công xâm nhập hệ thống camera giám sát, đánh cắp dữ liệu, hạn chế thiệt hại xảy ra đồng thời phối hợp với lực lượng Công an đấu tranh, xử lý với các loại tội phạm trên.

2. Khẩn trương triển khai các biện pháp kỹ thuật để phòng chống hoạt động xâm nhập hệ thống camera: *(1)* Thay đổi mật khẩu mặc định ngay khi lắp đặt; thiết lập mật khẩu mạnh (*chữ in hoa, số, ký tự đặc biệt*), thay đổi mật khẩu định kỳ (*03 tháng*); sử dụng tường lửa, thiết lập các quy tắc truy cập chặt chẽ, tắt các cổng không cần thiết; chỉ mở truy cập từ xa khi thực sự cần và sử dụng VPN hoặc các kênh bảo mật; thường xuyên cập nhật phần mềm cho thiết bị camera; *(2)* Làm việc với các nhà cung cấp dịch vụ viễn thông, đơn vị lắp đặt camera yêu cầu nâng cao trách nhiệm trong việc bảo mật thông tin, thực hiện quy trình bảo mật an toàn từ giai đoạn bàn giao thiết bị; yêu cầu các đơn vị này rà soát định kỳ, khắc phục các lỗ hổng bảo mật trên hệ thống máy chủ lưu trữ của camera (nếu có), các thiết bị camera mua sắm ưu tiên lựa chọn thương hiệu uy tín trong nước, có chính sách bảo mật và cập nhật rõ ràng; *(3)* Tách biệt mạng camera (IoT) với mạng làm việc chính bằng VLAN; *(4)* Không lắp đặt camera tại các khu vực nhạy cảm nếu không cần thiết, hoặc sử dụng chức năng che chắn vật lý khi không sử dụng.

3. Ban Tuyên giáo và Dân vận Tỉnh ủy, Sở Khoa học và Công nghệ tỉnh Lạng Sơn chỉ đạo các cơ quan thông tấn, báo chí, phát thanh truyền hình trên địa bàn tăng cường phối hợp đăng tải tin, bài trên các phương tiện thông tin đại chúng, phổ biến, chia sẻ trên các trang mạng xã hội về phương thức, thủ đoạn của các đối tượng sử dụng công nghệ cao tấn công xâm nhập hệ thống camera giám sát, đánh cắp dữ liệu và biện pháp phòng tránh, xử lý.

4. Các cơ quan, đơn vị, doanh nghiệp tổ chức phổ biến, quán triệt tới toàn thể cán bộ, công nhân viên, người lao động đặc biệt là những cán bộ, công nhân viên làm việc tại bộ phận công nghệ thông tin về phương thức, thủ đoạn

của các đối tượng sử dụng công nghệ cao đối tượng tấn công xâm nhập hệ thống camera giám sát, đánh cắp dữ liệu như trên để nâng cao cảnh giác, phòng ngừa và ngăn chặn thiệt hại.

Công an tỉnh Lạng Sơn thông báo và đề nghị các cơ quan, đơn vị trên địa bàn phối hợp, tổ chức thực hiện nghiêm túc./.

Nơi nhận:
- Như trên;
- Lưu: VT, PA05.

GIÁM ĐỐC

Thượng tá Vũ Thanh Tùng