UỶ BAN NHÂN DÂN **TỈNH THANH HÓA**	**CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 13228 /UBND-KSTTHCNC V/v đảm an ninh mạng, phòng ngừa lộ, mất thông tin, dữ liệu nội bộ, dữ liệu cá nhân trên môi trường mạng.	*Thanh Hoá, ngày* 10 *tháng* 9 *năm 2024*

Kính gửi:
- Các sở, ban, ngành, đơn vị cấp tỉnh;
- UBND các huyện, thị xã, thành phố.

Qua báo cáo của Công an tỉnh về công tác bảo đảm an ninh mạng trên địa bàn tỉnh thời gian qua, đã phát hiện một số sơ hở, thiếu sót trong việc bảo đảm an ninh, an toàn tài khoản được cấp cho các phần mềm, ứng dụng trong Hệ thống đăng nhập tập trung của tỉnh, dẫn đến bị lộ, mất thông tin đăng nhập và được chia sẻ trên một số diễn đàn của tin tặc trên thế giới; cụ thể:

(i) Một số đơn vị thiếu quy định, cơ chế quản lý, cấp phát, giám sát quá trình hoạt động sử dụng tài khoản trên các hệ thống, phần mềm dùng chung của tỉnh; chưa xác định, cụ thể hóa trách nhiệm và chế tài xử lý đối với từng tập thể, cá nhân được giao quản lý, sử dụng tài khoản khi để xảy ra sự cố gây mất an ninh, an toàn tài khoản; chưa có biện pháp bảo đảm an toàn đối với tài khoản của người dùng.

(ii) Cán bộ được giao quản lý, sử dụng tài khoản chưa thực hiện, tuân thủ các quy định về an toàn, an ninh thông tin mạng[1]; chưa thay đổi mật khẩu mặc định sau khi đăng nhập thành công lần đầu theo quy định; sử dụng mật khẩu mặc định với chuỗi ký tự đơn giản, dễ đoán; lưu thông tin đăng nhập tài khoản trên trình duyệt trong khi máy tính bị nhiễm mã độc, phần mềm độc hại có tính năng đánh cắp thông tin người dùng,… dẫn đến tài khoản dễ bị lộ, mất trên môi trường mạng.

(iii) Các đối tượng xấu, hacker sử dụng các phần mềm độc hại dạng "Stealer" và "Add-on" có tính năng thu thập thông tin (Xem tại *"Phụ lục: Các dạng phần mềm độc hại có tính năng thu thập dữ liệu và dấu hiệu nhận biết"* kèm theo văn bản này) để tấn công mạng, đánh cắp thông tin, dữ liệu nội bộ của các cơ quan, đơn vị và dữ liệu cá nhân.

Tình trạng trên dẫn đến nguy cơ cao bị lộ, mất bí mật nhà nước, bí mật nội bộ, thông tin cá nhân; bị các đối xấu lợi dụng khai thác, chiếm đoạt nhằm mục đích xấu, gây phức tạp về an ninh chính trị, trật tự an toàn xã hội trên địa bàn

---

[1] Điều 20 *"Quy chế tiếp nhận, xử lý, phát hành, quản lý và lưu trữ văn bản điện tử qua hệ thống phần mềm quản lý văn bản và hồ sơ công việc trong các cơ quan nhà nước trên địa bàn tỉnh Thanh Hóa"* ban hành kèm theo Quyết định 20/2019/QĐ-UBND ngày 26/6/2019 của UBND tỉnh.

tỉnh, đặc biệt là trong thời điểm chuẩn bị diễn ra Đại hội Đảng, bầu cử đại biểu Quốc hội và HĐND các cấp nhiệm kỳ 2026 - 2031.

Từ tình hình trên, để tăng cường các biện pháp bảo vệ bí mật nhà nước và thông tin, tài liệu nội bộ của cơ quan, đơn vị; bảo đảm an ninh, an toàn tài khoản sử dụng trong các phần mềm, ứng dụng dùng chung; phòng ngừa, ngăn chặn hoạt động tấn công mạng vào hệ thống thông tin trọng yếu của tỉnh và của các cơ quan, đơn vị, gây phức tạp về an ninh, trật tự trên địa bàn tỉnh, Chủ tịch UBND tỉnh, Trưởng Tiểu ban An toàn, an ninh mạng tỉnh[2] yêu cầu Giám đốc các sở, Thủ trưởng các ban, ngành, đơn vị cấp tỉnh, Chủ tịch UBND các huyện, thị xã, thành phố thực hiện nghiêm túc một số nội dung sau:

1. Tiếp tục phổ biến, quán triệt các quy định pháp luật về bảo đảm an toàn, an ninh mạng: Luật An ninh mạng, Nghị định số 53/2022/NĐ-CP ngày 15/8/2022 của Chính phủ quy định chi tiết một số điều của Luật An ninh mạng, Nghị định số 13/2023/NĐ-CP ngày 17/4/2023 của Chính phủ về bảo vệ dữ liệu cá nhân.

Quán triệt cán bộ, công chức, viên chức tuân thủ các quy định, quy chế về bảo vệ bí mật nhà nước, bí mật nội bộ trong đơn vị, thực hiện nghiêm "Quy chế tiếp nhận, xử lý, phát hành, quản lý và lưu trữ văn bản điện tử qua hệ thống phần mềm quản lý văn bản và hồ sơ công việc trong các cơ quan nhà nước trên địa bàn tỉnh Thanh Hóa" và các quy định liên quan. Cụ thể:

- Không lưu thông tin tài khoản Hệ thống đăng nhập tập trung, phần mềm, ứng dụng dùng chung của tỉnh, thư điện tử công vụ,... trên trình duyệt và trên máy tính, tránh trường hợp bị các đối tượng sử dụng phần mềm độc hại bí mật thu thập nhằm thực hiện các mục đích xấu.

- Thiết lập cơ chế kiểm soát truy cập trên các thiết bị, máy tính sử dụng trong hoạt động xử lý văn bản điện tử để hạn chế việc truy cập trái phép thông tin, dữ liệu nội bộ, dữ liệu cá nhân; trong đó, bao gồm việc sử dụng mật khẩu mạnh và phân quyền truy cập trên thiết bị, máy tính.

- Thận trọng trước khi tải xuống các ứng dụng và tài liệu, biểu mẫu văn bản trên mạng, không cài đặt các ứng dụng không cần thiết hoặc không liên quan đến công tác chuyên môn, đặc biệt là từ những nguồn không bảo đảm độ tin cậy để tránh bị lây nhiễm phần mềm độc hại.

- Thiết lập tường lửa mềm trên máy tính để chặn lọc lưu lượng mạng đáng ngờ từ các địa chỉ IP bên ngoài, có nguy cơ là các địa chỉ máy chủ điều khiển phần mềm độc hại.

- Thường xuyên rà quét mã độc, virus máy tính bằng các công cụ bảo mật uy tín, được cơ quan chức năng khuyến cáo.

---

[2] Quyết định số 409/QĐ-UBND ngày 18/7/2024 của UBND tỉnh.

2. Rà soát, bổ sung, ban hành cơ chế nhằm cụ thể hóa, xác định rõ trách nhiệm của tập thể và cá nhân trong bảo vệ bí mật nhà nước, bí mật nội bộ, quản lý, sử dụng và bảo đảm an ninh, an toàn tài khoản được cấp trên Hệ thống đăng nhập tập trung và các phần mềm ứng dụng dùng chung của tỉnh, thư điện tử công vụ, chữ ký số chuyên dùng... Quy định cụ thể chế tài xử lý trách nhiệm đối với tập thể, cá nhân khi để xảy ra sự cố mất an toàn thông tin mạng, lộ, mất tài khoản cấp cho đơn vị, cá nhân do nguyên nhân chủ quan không tuân thủ quy định về bảo đảm an ninh, an toàn thông tin mạng trong quá trình quản lý, sử dụng tài khoản.

3. Thực hiện cơ chế ghi nhật ký hoạt động (logfile) của từng tài khoản phục vụ công tác theo dõi định kỳ và kiểm tra, xác minh của các cơ quan chức năng khi có yêu cầu.

4. Định kỳ hoặc đột xuất tiến hành kiểm tra, đánh giá công tác bảo đảm an ninh mạng, an toàn thông tin, bảo vệ bí mật nhà nước trong đơn vị, bảo đảm việc thực hiện, chấp hành nghiêm túc. Thực hiện nghiêm các nội dung chỉ đạo của Trưởng Tiểu ban An toàn, An ninh mạng tỉnh, thông báo, cảnh báo, hướng dẫn của Công an tỉnh và Sở Thông tin và Truyền thông về các loại hình tấn công mạng, tội phạm mạng, tội phạm sử dụng công nghệ cao, các nguy cơ gây mất an toàn, an ninh mạng, lộ, mất bí mật nhà nước và lộ, mất thông tin, dữ liệu nội bộ và dữ liệu cá nhân.

5. Thủ trưởng các đơn vị chịu trách nhiệm trước Chủ tịch UBND tỉnh nếu để xảy ra tình trạng buông lỏng quản lý, gây mất an toàn thông tin mạng, lộ, mất bí mật nhà nước, thông tin tài khoản trên Hệ thống đăng nhập tập trung, thư điện tử công vụ và các phần mềm, ứng dụng dùng chung của tỉnh, chữ ký số…

6. Giao Công an tỉnh - Cơ quan Thường trực Tiểu ban An toàn, an ninh mạng tỉnh chủ trì, phối hợp với Sở Thông tin và Truyền thông định kỳ hoặc đột xuất kiểm tra việc thực hiện của các đơn vị; tổng hợp báo cáo và kịp thời tham mưu, đề xuất với Chủ tịch UBND tỉnh biện pháp chỉ đạo, xử lý trách nhiệm các tập thể, cá nhân có liên quan theo quy định./.

Nơi nhận:
- Như trên;
- Thường trực: Tỉnh ủy, HĐND tỉnh (để b/c);
- VP BCĐ An toàn, An ninh mạng quốc gia;
- Văn phòng: Tỉnh ủy, Đoàn ĐBQH và HĐND tỉnh, UBND tỉnh;
- Công an tỉnh;
- Lưu: VT, CNTT, KSTTHCNC.

KT. CHỦ TỊCH
PHÓ CHỦ TỊCH

Mai Xuân Liêm

Phụ lục: Các dạng phần mềm độc hại có tính năng thu thập dữ liệu và dấu hiệu nhận biết

(Kèm theo Văn bản số 13228/UBND-KSTTHCNC ngày 10 / 9 /2024 của UBND tỉnh)

1. Các loại phần mềm độc hại phổ biến có tính năng đánh cắp thông tin người dùng

a) **Stealer:** là một loại phần mềm độc hại (malware) được thiết kế để thu thập và đánh cắp thông tin từ các hệ thống bị lây nhiễm. Thông tin mà "Stealer" nhắm đến rất đa dạng tùy vào mục đích của kẻ tấn công[3], một số dòng "Stealer" còn được thiết kế riêng cho việc tấn công có chủ đích (APT) vào hệ thống thông tin quan trọng của các cơ quan chính phủ, hệ thống dịch vụ công quốc gia... Chúng hoạt động bằng cách xâm nhập vào hệ thống, thu thập dữ liệu và gửi thông tin về cho kẻ tấn công thông qua các máy chủ từ xa để ra lệnh và điều khiển hoạt động theo ý muốn.

b) **Add-on:** *(một số trình duyệt còn gọi là "Extension ")* là phần mềm chạy trên trình duyệt web với mục đích cải thiện các chức năng sẵn có của trình duyệt hoặc thêm mới các tiện ích giúp cho việc duyệt web được tốt hơn. Thông thường, "add-on" được chia làm 02 loại, gồm loại có thể tải về từ kho ứng dụng *(như Chrome Web Store)*, được bảo đảm về mức độ an toàn; loại còn lại được tải về từ các nguồn thứ ba không uy tín, khi cài đặt có nguy bị lây nhiễm mã độc và lấy cắp thông tin. Tuy nhiên, thời gian gần đây ghi nhận nhiều "add-on" tải về từ các kho ứng dụng đã bị các đối tượng cung cấp cố ý chèn mã độc hại vào để thực hiện các hành vi đánh cắp thông tin người dùng. Đáng chú ý, đây đều là những "addon" được nhiều người tải về để sử dụng trong thời gian dài, chỉ khi có cảnh báo từ các tổ chức uy tín về an ninh mạng thì các kho ứng dụng mới tiến hành rà soát, gỡ bỏ[4].

Quá trình người dùng sử dụng trình duyệt web, các "add-on" độc hại sẽ ghi nhận tất cả trình tự phím được gõ và các thông tin người dùng nhập vào các "web form" để đăng nhập tài khoản trên các trang mạng, đồng thời có thể chạy các tác vụ ác ý gây tổn hại hệ thống như đào tiền điện tử, khai thác trái phép tài nguyên máy tính, xóa dữ liệu... Bên cạnh đó, việc lưu thông tin đăng nhập tài khoản trên trình duyệt web dễ bị các phần mềm độc hại thu thập và lấy cắp thông tin hơn.

---

[3] Một số loại thông tin, dữ liệu các đối tượng thường nhắm đến là thông tin tài khoản từ các dịch vụ hoạt động trên môi trường mạng, mật khẩu, thẻ tín dụng, ví tiền điện tử, thông tin đăng nhập được lưu trên trình duyệt, thông tin hoạt động nội bộ của cơ quan, đơn vị, thông tin riêng tư của cá nhân...

[4] Đa số các "add-on" này đều được quảng bá với các tính năng hấp dẫn, phù hợp nhu cầu của đa số người dùng như hỗ trợ tải file, hỗ trợ tắt quảng cáo youtube, hỗ trợ săn giảm giá khi mùa hàng, duyệt web an toàn... Tuy nhiên đây chỉ là tính năng trá hình để che giấu mục dích là thu thập thông tin người sử dụng. Lưu ý, Tất cả các trình duyệt như Chrome, Firefox... chỉ gỡ bỏ các "add-on" độc hại trên kho ứng dụng, người dùng phải tự rà soát và tự gỡ trên trình duyệt nếu không các đối tượng xấu vẫn có thể tiếp tục khai thác và lấy cắp thông tin.

Hiện nay, hầu hết các phần mềm độc hại thuộc 02 hình thức nói trên trên đều được xây dựng và phân phối bởi các nhóm tin tặc hoạt động có tổ chức, với phương thức, thủ đoạn hết sức tinh vi; các đối tượng liên tục cải tiến, cập nhật chức năng, đa dạng hóa các biến thể của phần mềm nhằm khai thác triệt để thông tin, tài liệu nhạy cảm, bí mật lưu trữ trên máy tính, thiết bị của các cơ quan, đơn vị (trong đó có thông tin đăng nhập của các tài khoản phần mềm dùng chung của UBND tỉnh, tài khoản thư điện tử công vụ, tài khoản email, tài khoản ngân hàng ...) và tự động loại bỏ tung tích hoạt động, gây khó khăn cho công tác điều tra, truy vết của các đơn vị chức năng. Từ đó dẫn đến nguy cơ mất an toàn, an ninh mạng nghiêm trọng trên địa bàn tỉnh, như:

(1) Các đối tượng chia sẻ, rao bán thông tin công khai trên môi trường mạng hoặc sử dụng vào mục đích xấu, vi phạm pháp luật làm ảnh hưởng đến uy tín, hình ảnh của cơ quan, đơn vị.

(2) Lợi dụng thông tin có được làm bàn đạp tiến hành thâm nhập, tấn công leo thang các hệ thống thông tin vận hành phần mềm dùng chung trên địa bàn tỉnh để phá hoại, làm ngưng trệ hoạt động của hệ thống.

(3) Chiếm quyền sử dụng tài khoản, giả danh cán bộ, viên chức tại các sở, ban, ngành để can thiệp các hoạt động nội bộ và liên ngành (*như gửi, nhận văn bản điện tử tùy ý, gửi tài liệu chứa nội dung độc hại* ...) ảnh hưởng nghiêm trọng đến công tác điều hành, quản lý nhà nước nói chung trên địa bàn tỉnh.

(4) Gây thiệt hại về lợi ích về kinh tế trong trường hợp các đối tượng có được thông tin về giao dịch tài chính, tài khoản ngân hàng, tài sản trí tuệ... của cơ quan, tổ chức, cá nhân để bán lại cho bên thứ ba hoặc trực tiếp sử dụng vào mục đích xấu.

2. Dấu hiệu nhận biết

- *Hệ thống chậm bất thường:* Hiệu suất hệ thống suy giảm, ví dụ như khởi động máy mất nhiều thời gian, thời gian phản hồi ứng dụng chậm là do các phần mềm độc hại "Stealer" này thường chạy ở chế độ nền, liên tục gửi nhận dữ liệu ra bên ngoài hoặc đóng gói dữ liệu cục bộ trên máy tính để gửi định kỳ *(có thể thực hiện thêm thao tác mã hóa và ẩn dữ liệu để tránh bị phát hiện),* cá biệt một số phần mềm độc hại còn thực hiện thêm các hành vi khai thác tài nguyên hệ thống như đào tiền điện tử... đây đều là những hành vi làm tiêu tốn tài nguyên hệ thống và ảnh hưởng đến hiệu suất chung.

- *Hoạt động mạng đáng ngờ:* Một số phần mềm độc hại hoạt động rất tinh vi và không sử dụng quá nhiều tài nguyên hệ thống nhằm tránh việc bị phát hiện. Tuy nhiên, người sử dụng cần chú ý đến hành vi mạng bất thường, chẳng hạn lưu lượng sử dụng dữ liệu mạng gia tăng, ảnh hưởng đến các hoạt động sử dụng Internet khác, kết nối đáng ngờ đến các địa chỉ IP lạ,... Lý do là các phần mềm độc hại đánh cắp thông tin cần liên tục hoặc định kỳ giao tiếp với máy chủ điều khiển để gửi dữ liệu trên máy về cho các đối tượng tin tặc.

- *Các thiết lập trên trình duyệt web bị thay đổi:* "Stealer" và các "Add-on" độc hại thường nhắm vào trình duyệt web để đánh cắp thông tin nhạy cảm, chẳng hạn như mật khẩu và cookie trình duyệt. Nếu người sử dụng nhận thấy những thay đổi bất thường trong các thiết lập của trình duyệt, chẳng hạn như trang chủ mặc định, công cụ tìm kiếm mặc định hoặc "Add-on" mới mà người dùng không cài đặt, thì đó có thể là dấu hiệu của trình duyệt web bị xâm phạm. Bên cạnh đó, việc trình duyệt tự động đăng xuất ra khỏi tất cả các tài khoản mạng đã đăng nhập trước đó mà không do chủ ý của người dùng thì cần cảnh giác, rà soát lại trước khi thực hiện việc điền lại các thông tin tài khoản nhằm tránh bị các đối tượng tin tặc thu thập.

- *Các thông báo thể hiện hoạt động trái phép trên tài khoản:* Hầu hết các dịch vụ mạng hiện nay như Facebook, Google... đều gửi thông báo đến cho người sử dụng khi phát hiện có hành vi đăng nhập bất thường. Theo đó nếu nhận được các thông báo thể hiện việc đăng nhập bất thường qua thư điện tử, ứng dụng xác thực đa yếu tố hoặc tin nhắn điện thoại kèm mã số OTP (One-time Password), số dư tài khoản ngân hàng thay đổi bất thường thì có khả năng trước đó thiết bị của người sử dụng đã bị nhiễm phần mềm độc hại. Người dùng cần chú ý theo dõi hoạt động của tài khoản mạng và các thông báo về hành vi đáng ngờ. Khi xuất hiện các dấu hiệu trên cần thực hiện thay đổi mật khẩu và phương thức xác thực tài khoản.

3. Cơ chế lây nhiễm của "Stealer" và "Add-on" độc hại

- *Thông qua phần mềm, tài liệu, thư điện tử không an toàn:* Người dùng có thể bị nhiễm "Stealer" và "Add-on" độc hại khi tải xuống và cài đặt các phần mềm hoặc mở các tập tin tài liệu tải về từ các trang web, liên kết không đảm bảo độ tin cậy. Các phần mềm và tập tin này có thể được ngụy trang như để tỏ ra hữu ích hoặc phù hợp với nhu cầu của người dùng nhưng thực tế là được gắn kèm mã độc.

- *Thông qua các lỗ hổng bảo mật của hệ điều hành và phần mềm:* Phần mềm độc hại "Stealer" thường lợi dụng các lỗi bảo mật của hệ điều hành và các phần mềm đang tồn tại lỗ hổng bảo mật chưa được vá trên thiết bị để lây nhiễm mà không cần thao tác khác của người dùng.

- *Thông qua kết nối USB và thiết bị ngoại vi:* Phần mềm độc hại "Stealer" có thể lây nhiễm qua các thiết bị lưu trữ như USB khi người dùng kết nối chúng với máy tính mà không cài đặt trước phần mềm bảo mật để rà quét và ngăn chặn mã độc./.