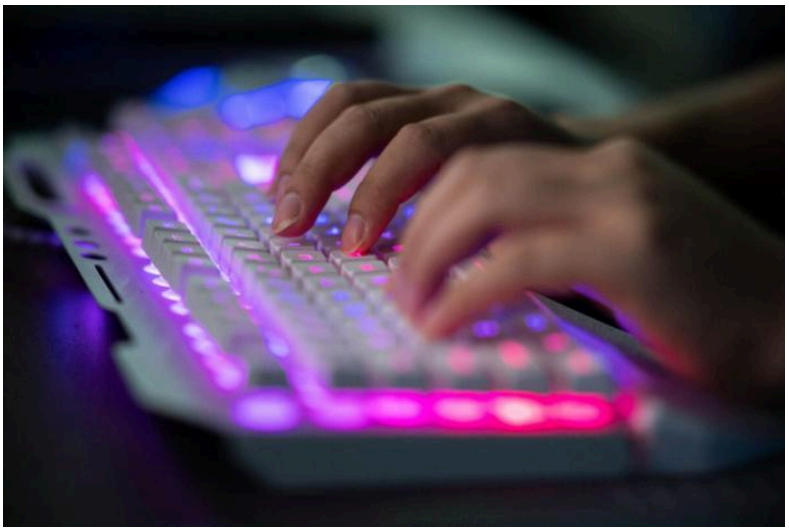
Trung Quốc có thể đang khai thác quy trình bảo mật Internet để đánh cắp dữ liệu

China Could Be Exploiting Internet Security Process to Steal Data, Cyber Experts Warn

By J.M. Phelps

Hạo Văn biên dịch

17/10/2021



Một người đàn ông đang sử dụng máy điện toán ở Đông Hoản, tỉnh Quảng Đông, Trung Quốc, vào hôm 04/08/2020. (Ảnh: Nicolas Asfouri/AFP/Getty Images)

Các chuyên gia an ninh mạng đã cảnh báo rằng để truy cập dữ liệu từ những người dùng nhẹ dạ cả tin, Đảng Cộng sản Trung Quốc (ĐCSTQ) có thể đang khai thác một quy trình xác thực toàn cầu được cho là an toàn, nhưng trên thực tế thì không.

Mặc dù mã hóa vẫn là phương pháp được ưa chuộng để bảo mật dữ liệu kỹ thuật số và bảo vệ máy điện toán, nhưng trong một số trường hợp, chính các chứng chỉ kỹ thuật số được sử dụng để xác thực trên internet đang cho phép chính quyền Trung Quốc xâm nhập vào các mạng máy điện toán khác nhau và tiến hành phá hoại, các chuyên gia cho hay.

Các tổ chức trên khắp thế giới, được gọi là “các cơ quan cung cấp chứng chỉ” (CA), phát hành các chứng chỉ kỹ thuật số để xác minh danh tính của các tổ chức kỹ thuật số trên mạng internet.

Theo ông Andrew Jenkinson, Giám đốc Điều hành của công ty an ninh mạng Cybersec Innovation Partners (CIP) và là tác giả của cuốn sách “Stuxnet to Sunburst: 20 Years of Digital Exploitation and Cyber Warfare”, một chứng chỉ kỹ thuật số có thể được so sánh như một hộ chiếu hay giấy phép lái xe vậy.

Ông Jenkinson nói với The Epoch Times, “Nếu không có chứng chỉ kỹ thuật số, người hoặc thiết bị họ đang sử dụng không thể theo các tiêu chuẩn công nghiệp, và việc mã hóa dữ liệu cốt yếu có thể bị bỏ qua, chỉ còn lại những gì được cho là được mã hóa ở dạng văn bản thuần túy”.

Thông qua mật mã, các chứng chỉ kỹ thuật số được sử dụng để mã hóa thông tin liên lạc giữa nội bộ và bên ngoài nhằm ngăn chặn tin tặc, chẳng hạn như, khỏi việc bị chặn và đánh cắp dữ liệu. Nhưng “chứng chỉ giả mạo” hoặc không hợp lệ có thể thao túng toàn bộ quá trình mã hóa và kết quả là “mang lại cho hàng triệu người dùng một cảm giác an toàn giả”, ông Jenkinson nói.

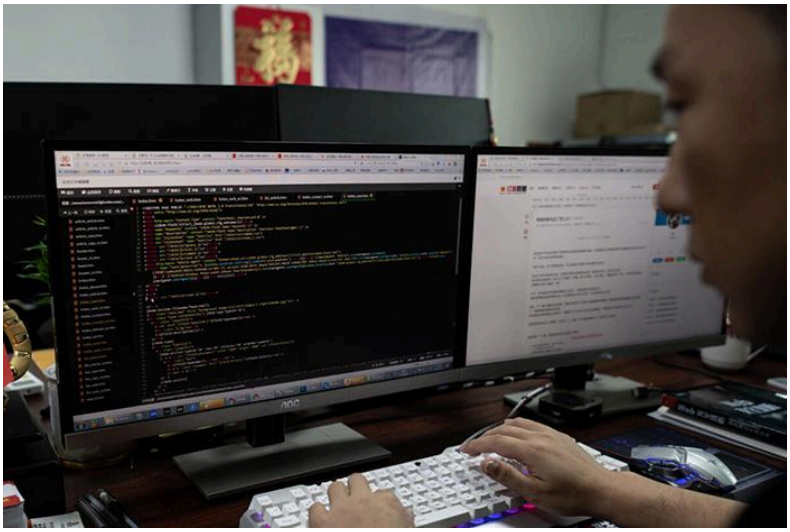
Các lớp của niềm tin giả

Ông Michael Duren, phó chủ tịch điều hành của công ty an ninh mạng Global Cyber Risk LLC, nói rằng chứng chỉ kỹ thuật số thường được cấp bởi các CA đáng tin cậy và mức độ tin cậy ngang hàng sau đó sẽ được chuyển cho các nhà cung cấp trung gian. Tuy nhiên, ở đây có cơ hội cho một tổ chức cộng sản, một kẻ xấu hoặc một tổ chức không đáng tin cậy khác cấp chứng chỉ cho “những kẻ bất chính” khác có vẻ là đáng tin cậy nhưng không phải vậy, ông nói.

“Khi một chứng chỉ được cấp từ một tổ chức đáng tin cậy, thì chứng chỉ đó sẽ được tin cậy”, ông Duren nói. “Nhưng những gì mà công ty phát hành thực sự có thể đã làm là trao sự tin tưởng đó cho một người không thể tin tưởng được”.

Ông Duren cho biết ông sẽ không bao giờ tin tưởng một cơ quan cấp chứng chỉ của Trung Quốc vì lý do này, nói rằng ông biết một số công ty đã cấm các chứng chỉ tiếng Trung vì chúng được cấp cho các tổ chức không thể tin cậy được.

Ông Jenkinson nói rằng các cơ quan cấp chứng chỉ của Trung Quốc chiếm một tỷ lệ nhỏ trong tổng thể ngành và các chứng chỉ mà họ cấp thường chỉ giới hạn ở các tổ chức và sản phẩm của Trung Quốc.



Prince, một thành viên của nhóm tin tặc Liên minh Tin tặc Đỏ (Red Hacker Alliance), đã từ chối cho biết tên thật của mình, đang sử dụng máy điện toán của mình tại văn phòng của nhóm này ở Đông Hoản, tỉnh Quảng Đông, Trung Quốc, hôm 04/08/2020 (Ảnh: Nicolas Asfouri/AFP/Getty Images)

Vào năm 2015, các chứng chỉ được cấp bởi Trung tâm Thông tin Mạng Internet Trung Quốc (CNNIC), cơ quan do nhà nước vận hành giám sát việc đăng ký tên miền của Trung Quốc, đã bị nghi ngờ. Google và Mozilla đã cấm các chứng chỉ CNNIC khi biết được các chứng chỉ kỹ

thuật số trái phép đã kết nối với một số miền. Cả hai công ty internet này đều đã phản đối việc CNNIC giao quyền cấp chứng chỉ cho một công ty Ai Cập, vốn là công ty đã cấp các chứng chỉ trái phép.

Theo ông Jenkinson, các chứng chỉ CNNIC đã bị cấm vì "chúng có cửa sau".

"Một cửa sau có nghĩa là [cơ quan cấp chứng chỉ Trung Quốc] có thể tiếp quản quyền quản trị và gửi dữ liệu trở lại quyền trung tâm", ông cho hay.

Kể từ năm 2016, Mozilla, Google, Apple và Microsoft cũng đã cấm Cơ quan cấp Chứng chỉ Trung Quốc WoSign và công ty con StartCom của họ vì các thông lệ bảo mật không được chấp nhận.

Lỗi an ninh

Bất chấp những lệnh cấm này đối với các chứng chỉ kỹ thuật số của Trung Quốc trong những năm gần đây, ĐCSTQ vẫn không hề nao núng và đang chơi một cuộc chơi dài hơi, ông Jenkinson cho biết.

Ông chỉ ra một phát hiện đáng báo động do công ty an ninh mạng của ông thực hiện cách đây hai năm, có ảnh hưởng đến một công ty tư vấn đa quốc gia.

Thông thường, các chứng chỉ kỹ thuật số có hiệu lực trong một vài năm, tùy thuộc vào tổ chức cấp chứng chỉ và việc gia hạn là bắt buộc để giữ cho chúng hợp lệ và dữ liệu mà chúng phải bảo vệ được an toàn, ông nói.

Ông Jenkinson nói, "Nhưng vào năm 2019, CIP Chinese đã phát hiện ra các chứng chỉ đã tồn tại trong 999 năm".

Công ty của ông đã phát hiện ra điều này khi kiểm tra các máy điện toán xách tay của một công ty tư vấn nổi tiếng toàn cầu.

Ông Jenkinson đã phản ánh lỗi bảo mật này để công ty này chú ý và đưa ra các dịch vụ để bảo mật máy điện toán và mạng của khách hàng. Nhưng công ty này đã từ chối.

“Hoặc là họ vô cùng tự mãn, hoặc là họ đồng lõa”, ông nói, lưu ý rằng khách hàng của công ty này bao gồm cả các tổ chức chính phủ Hoa Kỳ.

Ông Jenkinson nói, công ty trị giá hàng tỷ USD này không thể khắc phục được vấn đề này có nghĩa là hàng trăm ngàn người có thể bị ảnh hưởng bởi sự xâm nhập của Trung Quốc thông qua hệ thống bảo mật lỏng lẻo của công ty này.

Ông nói, công ty này đang gây tổn hại đến khách hàng của mình mỗi khi ai đó sử dụng một trong những máy điện toán xách tay của họ. Chẳng hạn, các công ty hoặc khách hàng sử dụng dịch vụ của công ty này có thể bị đòi tiền chuộc, bị đánh cắp tài sản trí tuệ, hoặc là nhận phải các mã độc được gài vào để sử dụng về sau này.

Công ty này “vi phạm mọi quy định về quyền riêng tư mà con người biết đến – và họ chỉ muốn bác bỏ điều đó”, chuyên gia an ninh mạng này cho hay, đặc biệt chỉ ra luật bảo vệ dữ liệu nghiêm ngặt của Liên minh Âu Châu.

Và nếu thông tin này được công khai, hậu quả sẽ rất lớn, ông Jenkinson cho biết.

“Hãy tưởng tượng một cuộc tấn công có chủ đích (waterhole attack) hoặc một cuộc tấn công không có chủ đích (drive-by attack), một cuộc tấn công mà trong đó tội phạm mạng có thể chỉ cần ngồi đó và dễ dàng có được quyền truy cập để thu thập dữ liệu mà không cần phải suy nghĩ hoặc phải giải mã nó – bởi vì tất cả đều ở dạng văn bản thuần túy [do chứng chỉ giả mạo hoặc lỗi cấu hình]”, ông nói.

Đối với một công ty có uy tín lớn như vậy lại lựa chọn không bảo vệ cho khách hàng của họ là điều “điên rồ”, ông Jenkinson cho hay.

Một ‘con dốc trơn trượt’

Theo ông Jenkinson, thiệt hại kinh tế do tội phạm mạng vẫn hoàn toàn chưa có thay đổi đúng hướng.

Theo báo cáo từ công ty bảo mật máy điện toán McAfee, thiệt hại toàn cầu do tội phạm mạng đã vượt quá 1 ngàn tỷ USD vào năm 2020. Công ty nghiên cứu Cybersecurity Ventures cho biết vào năm 2021, thiệt hại dự kiến sẽ leo thang lên hơn 6 ngàn tỷ USD.

Ông Jenkinson dự đoán rằng thiệt hại kinh tế sẽ vượt quá 10 ngàn tỷ USD vào năm 2025.

“Điều này sẽ ảnh hưởng đến mọi người đàn ông, phụ nữ và trẻ em. “Chà, chúng ta đang ở trên con dốc trơn trượt, chúng ta đang tự làm trơn nó”, ông nói

Ông Jenkinson cho hay, “Việc mọi người không nên sử dụng các chứng chỉ kỹ thuật số CNNIC như là một bước khởi đầu để đảo ngược xu hướng này”.

Ông Duren của Global Cyber Risk đồng tình với điều này, nói rằng, “Bất cứ điều gì đến từ một tổ chức do nhà nước kiểm soát như Trung Quốc cộng sản đóng vai trò là cơ quan cấp chứng thì chỉ đều không nên được tin tưởng.”

Ông Jenkinson nói rằng các CA cần kiểm soát và giám sát tốt hơn. “Nếu không có điều này, không ai có bất kỳ cơ hội nào để biết các chứng chỉ kỹ thuật số nào đang được sử dụng, vì một máy điện toán xách tay tiêu chuẩn chứa hàng trăm ngàn phiên bản chứng chỉ kỹ thuật số”.

Ông Jenkinson lưu ý rằng các sản phẩm máy điện toán của Trung Quốc sẽ chủ yếu sử dụng chứng chỉ kỹ thuật số của Trung Quốc. Do đó, người dùng các sản phẩm như vậy nên biết rằng hệ quả là sự bảo mật của họ có thể bị xâm phạm.

Ông J.M. Phelps là một nhà văn và nhà nghiên cứu về các mối đe dọa từ chủ nghĩa Hồi giáo cực đoan và Trung Quốc.

Hạo Văn biên dịch

Việt Luận Úc Châu